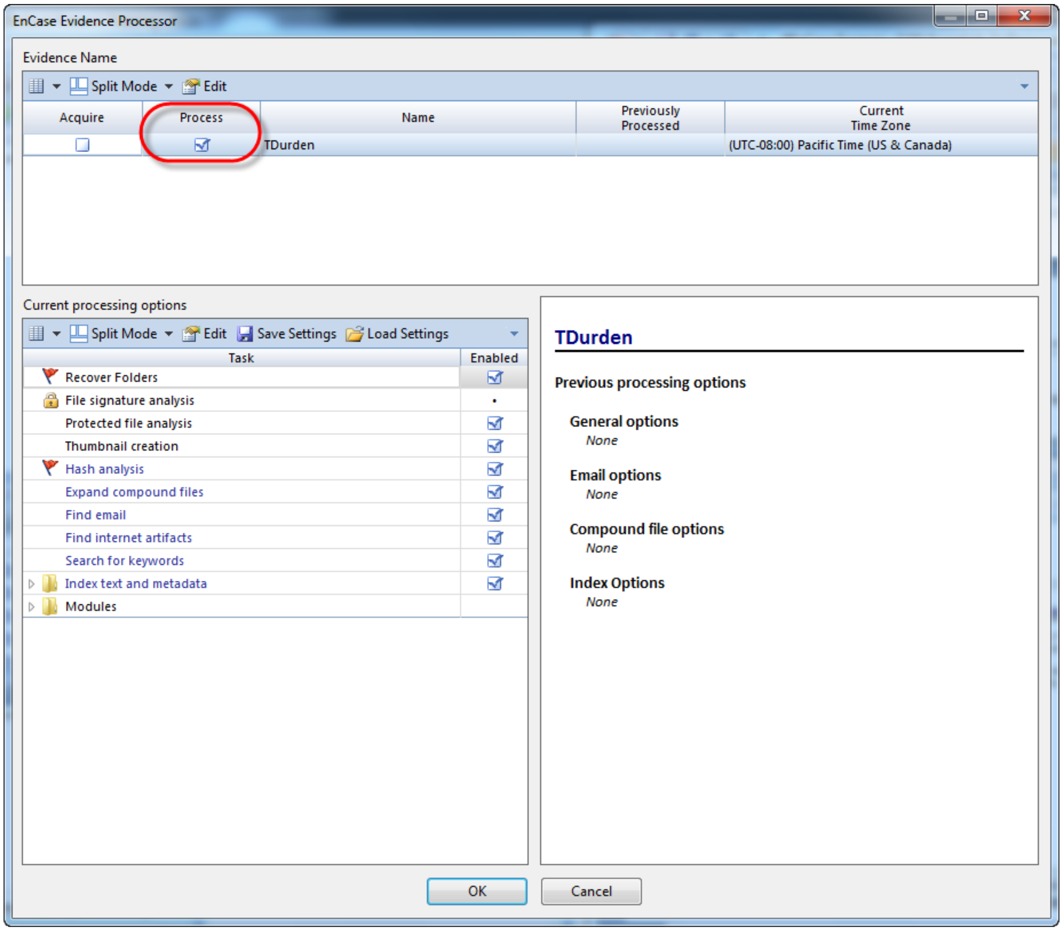
ATTACHED ATTACHMENTS
SUBMISSION OF COMPUTER FORENSIC SOFTWARE USER MANUALS
CR08-814-PHX-DGC

↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓
↓ ATTACHMENT 02 ↓

EnCase Forensic v7 Essentials Training OnDemand – v7.04.01i (06.06.2012), **part 2 of 3**; Note: manual broken up into three parts in order to keep attachments under 10mb for PACER.

Click the **Process** check box for the TDurden evidence file to enable the Evidence Processor Task list.



EnCase Evidence Processor

Evidence Name

Acquire	Process	Name	Previously Processed	Current Time Zone
□	☑	TDurden		(UTC-08:00) Pacific Time (US & Canada)

Current processing options

Task	Enabled
Recover Folders	☑
File signature analysis	•
Protected file analysis	☑
Thumbnail creation	☑
Hash analysis	☑
Expand compound files	☑
Find email	☑
Find internet artifacts	☑
Search for keywords	☑
Index text and metadata	☑
Modules	

TDurden

Previous processing options

General options
None

Email options
None

Compound file options
None

Index Options
None

Figure 5-14 Enable the Evidence Processor

A major benefit of the Evidence Processor is that its settings do not require your interaction during operation.

Functions with the lock cannot be changed or disabled. Functions with the red flag cannot be run at a future time on the evidence if they are not selected initially.

The following evidence processing functions are available:

- **Recover folders** – Recover files that have been deleted or corrupted on FAT and NTFS volumes
- **File signature analysis** – Determine if the extension of a file has been altered and whether or not the extension matches the file type as specified by the file's header
- **Protected file analysis** – Identify encrypted and password-protected files with the Passware Encryption Analyzer

- **Thumbnail creation** – Creates image thumbnails for faster display in the EnCase® GUI
- **Hash analysis** – Generate MD5 and/or SHA1 hash values for files and compare against your case Hash Library
- **Expand compound files** – Expand compound and compressed files, such as ZIP, RAR, GZ, and Windows registry archives
- **Find email** – Extract individual messages from e-mail archive files, such as PST (Microsoft® Outlook), NSF (Lotus® Notes), DBX (Microsoft® Outlook Express), EDB (Microsoft® Exchange), AOL, and MBOX.
- **Find internet artifacts** – Collect Internet-related artifacts, such as browser histories and cached web pages. You also have the option to search unallocated space for the Internet artifacts.
- **Search for keywords** – Search raw (not transcript) text for specific keywords.
- **Index text and metadata** – Create an index for when you need to search for keywords in compound files (Microsoft Office 2007 and 2010) and across large amounts of data. You can adjust the parameters for index creation, such as the minimum word length to index and whether to use a noise file (which does not index specific and common words).

The Evidence Processor contains numerous useful features:

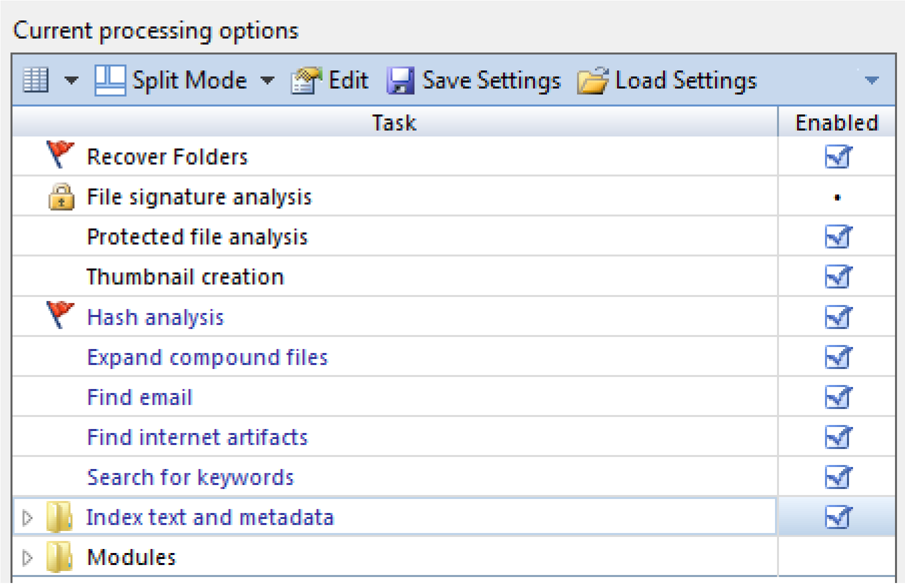
- The simultaneous processing of multiple devices
- The convenience of acquiring devices right from the Evidence Processor
- Saving sets of Evidence Processor options as templates to be run with little or no modification at a later date
- The ability to be run from the command line
- On-screen instructions that guide you through the use of each setting
- Automatic processing of the results from any EnScript modules according to the current processor settings (Index, Keyword search, etc.)

Evidence Processing Tasks

Use the Evidence Processor pane to select the processing tasks to configure and run.

To select an option, click its **Enable** checkbox:

- If a task name is listed in a ***blue*** font, click on its task name to configure it
- If a task name is listed in a ***black*** font, no further configuration is necessary



Task	Enabled
Recover Folders	☑
File signature analysis	•
Protected file analysis	☑
Thumbnail creation	☑
Hash analysis	☑
Expand compound files	☑
Find email	☑
Find internet artifacts	☑
Search for keywords	☑
Index text and metadata	☑
Modules	

Figure 5-15 Evidence Processor tasks

Recover Folders

Running the Recover Folders task on FAT partitions will search through the unallocated clusters of a specific FAT partition for the “dot, double-dot” signature of a deleted folder. When the signature matches, EnCase v7 can rebuild files and folders that were within the deleted folder.

This task can recover NTFS files and folders from unallocated clusters and continue to parse through the current Master File Table (MFT) records for files without parent folders. This operation is particularly useful when a drive has been reformatted or the MFT is corrupted. Recovered files are placed in the gray Recovered Folders virtual folder in the root of the NTFS partition.

File Signature Analysis

A common technique used to hide data and disguise the true nature of a file is to rename the file and change its extension; for example, renaming an image file with a .jpg extension to a file with a .dll extension, which is not associated with a graphics file.

This process will determine whether the extension of a file has been modified and whether it matches the type of file that is specified by the file's header bytes. The process is not user-configurable and is always enabled because it is necessary to support other operations within EnCase v7.

Protected File Analysis

Encrypted and password-protected files are frequently good ways to hide data. The Evidence Processor's protected file analysis process uses the Passware Encryption Analyzer (http://www.lostpassword.com/encryption-analyzer.htm) to identify these types of files and information about the application used to protect them.

Starting with Passware 11.7, you can export the index and known passwords as a dictionary used for decrypting protected files. Using this feature requires a valid installation of the Passware Kit.

Thumbnail Creation

By default, the Evidence Processor generates thumbnails for all image files and stores them as part of the cache.

Because thumbnails are smaller and load faster, generating thumbnails significantly improves the speed with which you can work with pictures in EnCase v7.

Hash Analysis

A hash is a digital fingerprint of a file or collection of data, commonly represented as a string of binary data written in hexadecimal notation. In EnCase v7, it is the result of a hash function run against any mounted drive, partition, file, or chunk of data. The most common uses for hashes are to:

- Identify when a chunk of data changes, which frequently indicates evidence tampering
- Verify that data has not changed in which case the hash should be the same both before and after the verification
- Compare a hash value against a library of known good and bad hashes, seeking a match

The Evidence Processor's hash analysis setting allows you to create MD5 and SHA-1 hash values for files, so that you can later use them for the reasons specified previously. When you click the **Hash Analysis** hyperlinked name, the Edit Settings dialog appears, allowing you to check whether to run either or both of these hashing algorithms.

Expand Compound Files

Use this setting to expand archive files, including .zip and .rar files, and/or registry archives.

For archive files, EnCase v7 will extract the compressed or archived files and process them, according to the other Evidence Processor settings that you have chosen. This includes nested archive files or zip files within a zip file.

Find E-mail

Select this setting to extract individual messages from e-mail archives.

To select the e-mail archive types to search for messages:

1. Click **Find Email**
2. Click the e-mail archive file types whose messages you want to examine and click **OK**
3. Check the **Search for Additional Lost or Deleted Items** box for a search for deleted e-mails

After processing is completed, EnCase v7 can analyze the component files extracted from the archives, according to the other Evidence Processor settings you selected.

Thread E-mail

By default, the Evidence Processor performs a thread analysis on e-mail messages that it processes.

Once your evidence has been processed, you can track the different e-mail threads and communication patterns among senders and receivers of the messages with the **Show conversation** and **Show related messages** e-mail features.

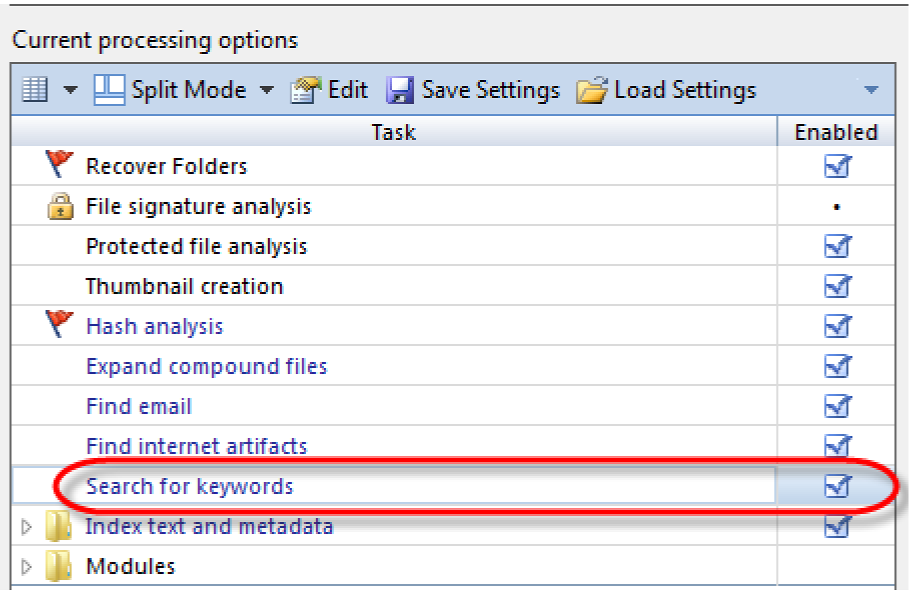
Find Internet Artifacts

Choose this Evidence Processor setting to find Internet-related artifacts, such as browser histories and cached web pages. You can also use this setting to search for Internet artifacts of various types within unallocated space.

Search for Keywords

Use this option to run a raw keyword search during the processing. Once you enable **Search for Keywords** by checking its box, the keyword list for the current case is displayed in the right panel.

NOTE: For faster results, it is recommended that the Raw Keyword search function outside the Evidence Processor be used. However the search function is provided to allow more automated processing before analysis.

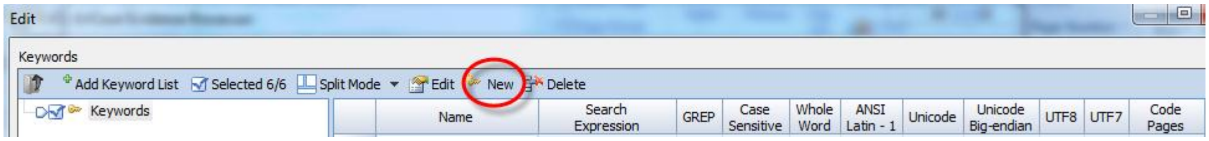


Current processing options

Task	Enabled
Recover Folders	☑
File signature analysis	•
Protected file analysis	☑
Thumbnail creation	☑
Hash analysis	☑
Expand compound files	☑
Find email	☑
Find internet artifacts	☑
Search for keywords	☑
Index text and metadata	☑
Modules	

Figure 5-16 Raw text search with keywords

To edit the keyword settings, click **Search for keywords**. The Edit keyword list dialog appears.



	Name	Search Expression	GREP	Case Sensitive	Whole Word	ANSI Latin - 1	Unicode	Unicode Big-endian	UTF8	UTF7	Code Pages

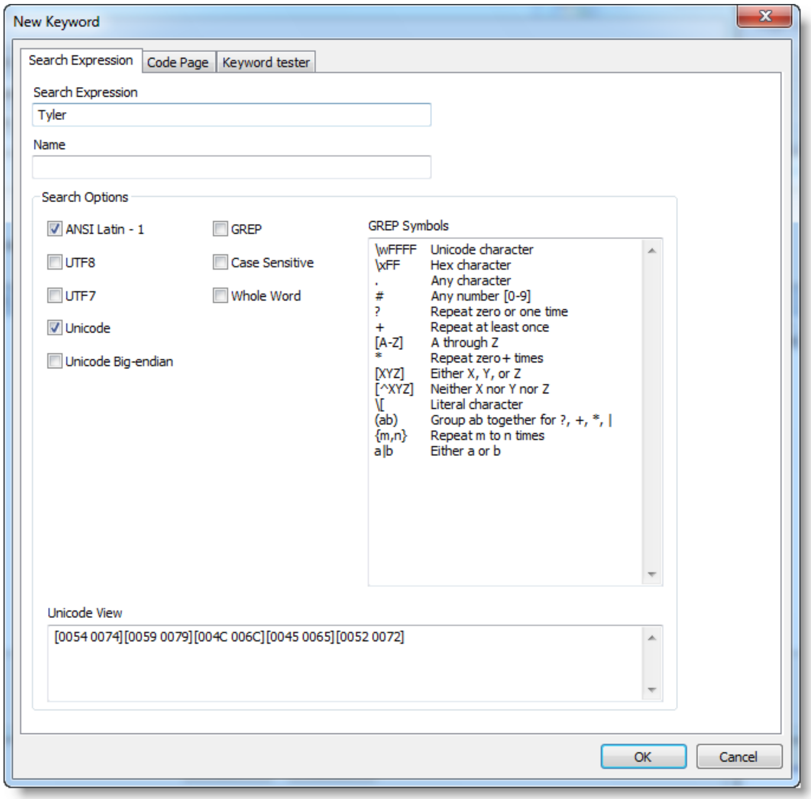
Figure 5-17 Edit keywords dialog

In the dialog, use the checkboxes and toolbar items to:

- Add a keywords list to a file
- Add new keywords
- Edit keywords
- Delete keywords
- Specify where and how to search
- Change the layout of the keyword table

New Keyword

To add a new keyword, click **New** in the Edit keyword dialog. The New Keyword dialog appears.



Search Expression: Tyler

Name:

☑ ANSI Latin - 1
□ UTF8
□ UTF7
☑ Unicode
□ Unicode Big-endian
□ GREP
□ Case Sensitive
□ Whole Word

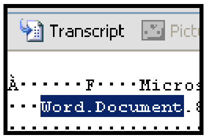
\wFFFF	Unicode character
\xFF	Hex character
.	Any character
#	Any number [0-9]
?	Repeat zero or one time
+	Repeat at least once
[A-Z]	A through Z
*	Repeat zero+ times
[XYZ]	Either X, Y, or Z
[^XYZ]	Neither X nor Y nor Z
\[	Literal character
(ab)	Group ab together for ?, +, *, |
{m,n}	Repeat m to n times
a|b	Either a or b

Unicode View: [0054 0074][0059 0079][004C 006C][0045 0065][0052 0072]

Figure 5-18 New Keyword dialog

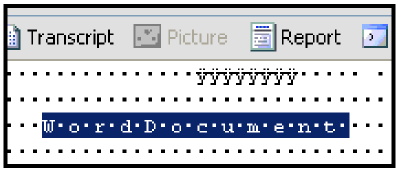
1. **Search Expression** – Enter your search expression in this box. It may be a simple keyword, phrase, or a GREP expression.
2. If you intend to search for keywords using a different character set, you may need to change the code page. In that case, click the **Code Page** tab, scroll through the list, and check the code page **Name** you want.
3. **Name** – Although not required, you may enter a descriptive name that will help you remember what the search expression is intended to search for. This is very useful with GREP search expressions and foreign language searches.
4. **Case Sensitive** – EnCase v7 will locate the keyword regardless of the individual characters' case unless this box is checked. If checked, EnCase v7 will only locate the keyword if the case sensitivity is the same as the search expression entered.
5. **GREP** – The GREP option must be selected when utilizing GREP search characters. GREP is used to narrow the search, limit false-positive search hits, and in those cases where only certain portions of the keyword being sought are known.

6. **ANSI Latin 1** – This default option will search for characters contained within the ANSI Latin-1 code page, which is the default code page for the Microsoft Windows operating system. In earlier versions of EnCase® software, this option was called "Active Code Page." Since the active code page varied according to the active code page enabled on your computer, this option was replaced by ANSI Latin-1 to ensure consistent results.
7. **Unicode** – Unicode was developed in direct response to foreign language character sets. Most MS Office products use Unicode as does Windows 2000, XP, Vista, and 7. Enabling both ANSI Latin-1 and Unicode options will locate both ASCII and Unicode characters. However selecting the Unicode option alone (without the ANSI Latin-1 option or appropriate code page selected) will find data stored in Unicode only. For more details on Unicode, please see http://www.unicode.org.



```
À······F····Micros
···Word.Document.
·····························
```

Figure 5-19 Example of plain text



```
···············ÿÿÿÿÿÿÿÿ·····  ·
······························
···W·o·r·d·D·o·c·u·m·e·n·t····
······························
```

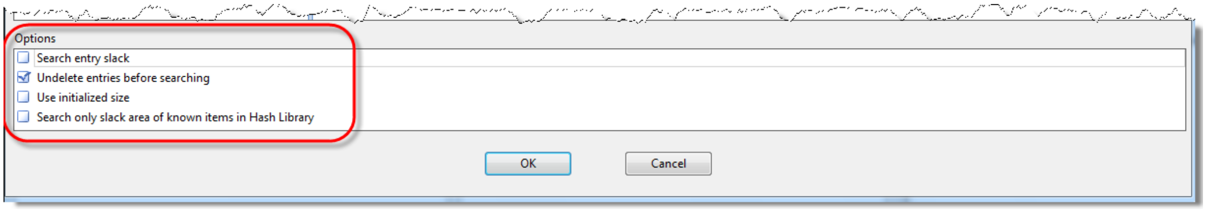
Figure 5-20 Example of Unicode

8. **Unicode Big-Endian** – Non-Intel based data formatting scheme that stores multiple-byte numerical values with the most significant byte values first, which is the reverse of little Endian.
9. **UTF-8** – UTF stands for Universal Character Set Transformation Format. Applications have several options for how they encode Unicode. The most common encoding is UTF-8, which is the 8-bit form of Unicode. This option offers foreign language support.
10. **UTF-7** – UTF-7 is a special format that encodes Unicode characters within US-ASCII in a way that all mail systems can accommodate.
11. **Whole Word** – EnCase v7will locate the keyword as a whole word not within a larger word (i.e., Chris not Christopher)

When finished, click **OK** to save the keyword in your case.

Other Keyword Search Options

- **Search entry slack** – This option tells EnCase v7 to search the slack area, which exists between the end of the logical data to the end of the physical file for all items searched.
- **Use initialized size** – This option tells EnCase v7 to search only the initialized size of an entry as opposed to the logical or physical size. When a file is opened on the NTFS file system, if the initialized size is smaller than the logical size, the space after the initialized size is zeroed out. Searching the initialized size searches only data a user would see within a file.
- **Undelete entries before searching** – This option will logically "undelete" deleted files prior to searching. If a file is deleted, EnCase v7 and other tools can determine if the assigned starting cluster is not currently assigned to another file (if it is assigned, then the file is deemed deleted/overwritten). The unallocated clusters after the starting cluster may or may not belong to the deleted file. Choosing this option assumes that the unallocated clusters after the starting cluster do belong to the deleted file. This is the same assumption made when copying out a deleted file. Choosing this option will find a keyword fragmented between the starting cluster and the subsequent unallocated cluster. If determining the presence of a keyword on the media is critical to an investigation, you should also search for portions of the keyword, including utilizing GREP search expressions for fragments of the keyword.
- **Search only slack area of entries in Hash Library** – This option is used in conjunction with a hash analysis. If a file is identified from the hash library, then it will not be searched. However the slack area behind the file (as described previously) will be searched. If this option is turned off, EnCase v7 will ignore the hash analysis.



Options

☐ Search entry slack
☑ Undelete entries before searching
☐ Use initialized size
☐ Search only slack area of known items in Hash Library

Figure 5-21 Search options

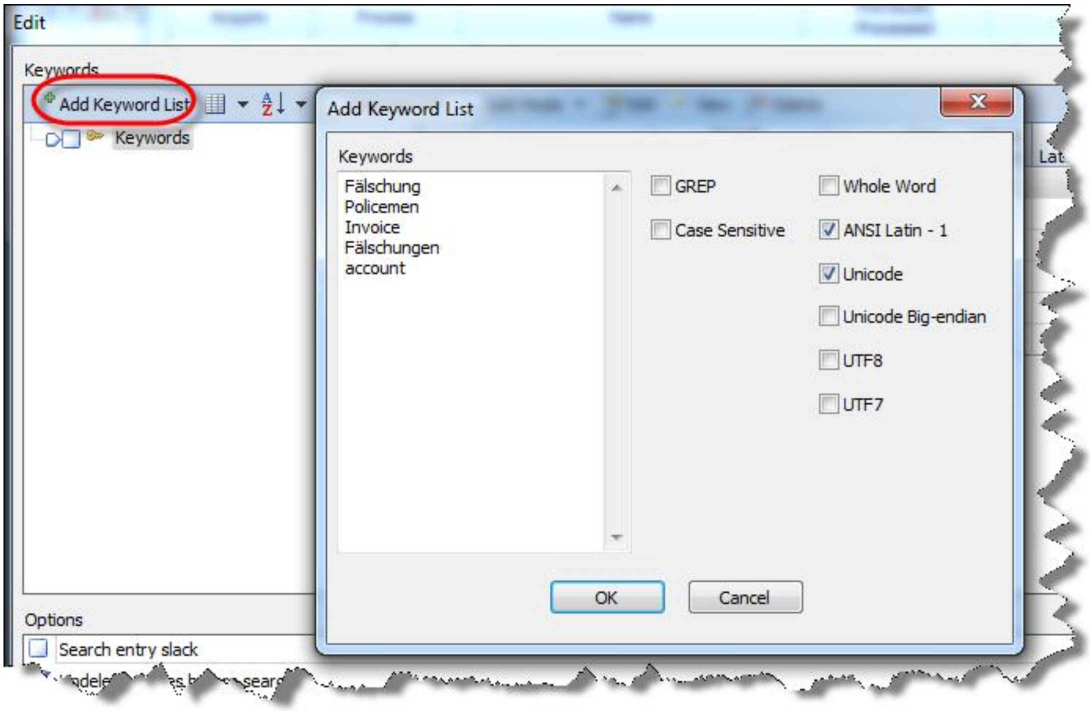
Additional Methods for Entering Keywords

Add Keyword List

To add a list of keywords, as opposed to adding one keyword at a time, select **Add Keyword List**. Keyword lists can be entered from the keyboard or pasted from a text document with one search expression and a line return per line. Options can be selected for all keywords and modified later if needed.

Example keywords include:

- Fälschung
- Policemen
- Invoice
- Fälschungen
- account

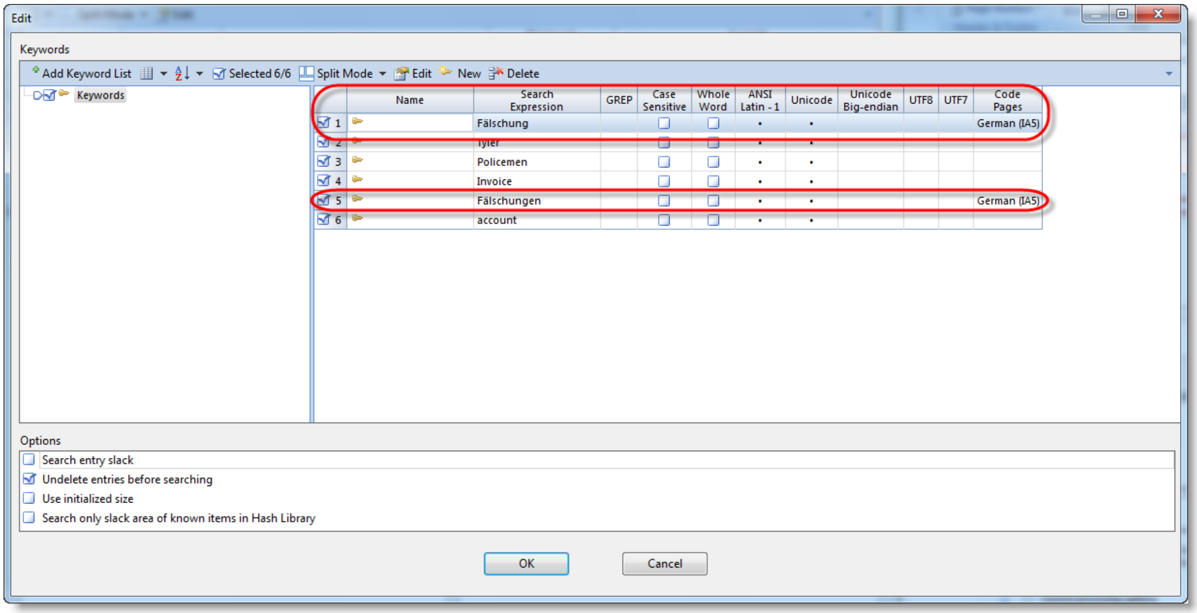


Keywords:
Fälschung
Policemen
Invoice
Fälschungen
account

□ GREP
□ Case Sensitive
□ Whole Word
☑ ANSI Latin - 1
☑ Unicode
□ Unicode Big-endian
□ UTF8
□ UTF7

Figure 5-22 Add Keyword List screen

You can edit individual keywords to add code pages.

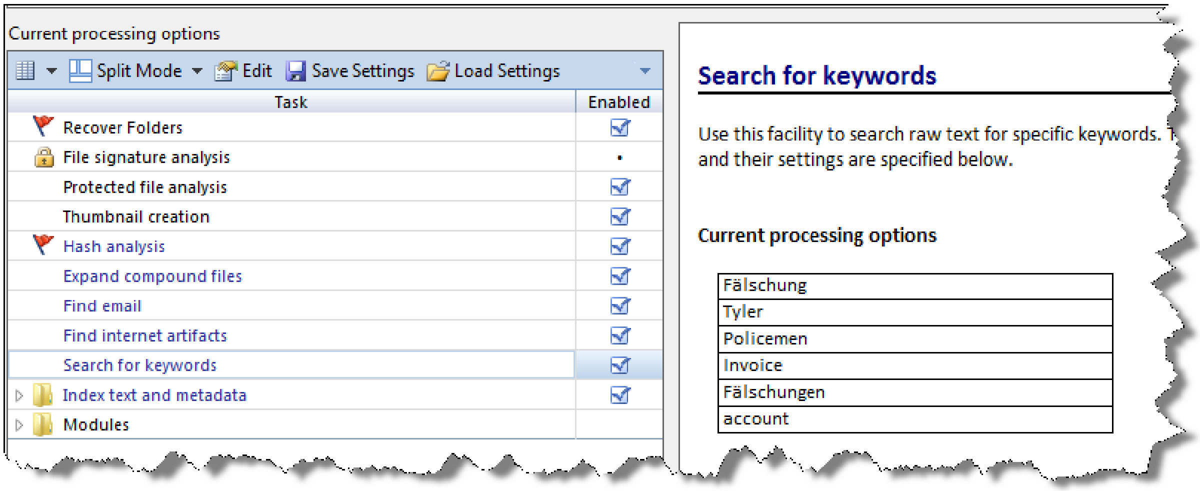


	Name	Search Expression	GREP	Case Sensitive	Whole Word	ANSI Latin - 1	Unicode	Unicode Big-endian	UTF8	UTF7	Code Pages
☑ 1		Fälschung		□	□	•	•				German (IA5)
☑ 2		Tyler		□	□	•	•				
☑ 3		Policemen		□	□	•	•				
☑ 4		Invoice		□	□	•	•				
☑ 5		Fälschungen		□	□	•	•				German (IA5)
☑ 6		account		□	□	•	•				

Options
- □ Search entry slack
- ☑ Undelete entries before searching
- □ Use initialized size
- □ Search only slack area of known items in Hash Library

Figure 5-23 Code Pages

When completed with the keyword editing, click **OK**.



Task	Enabled
Recover Folders	☑
File signature analysis	•
Protected file analysis	☑
Thumbnail creation	☑
Hash analysis	☑
Expand compound files	☑
Find email	☑
Find internet artifacts	☑
Search for keywords	☑
Index text and metadata	☑
Modules	

Search for keywords

Use this facility to search raw text for specific keywords. T
and their settings are specified below.

Current processing options

Fälschung
Tyler
Policemen
Invoice
Fälschungen
account

Figure 5-24 Current keyword options

Index Text and Metadata

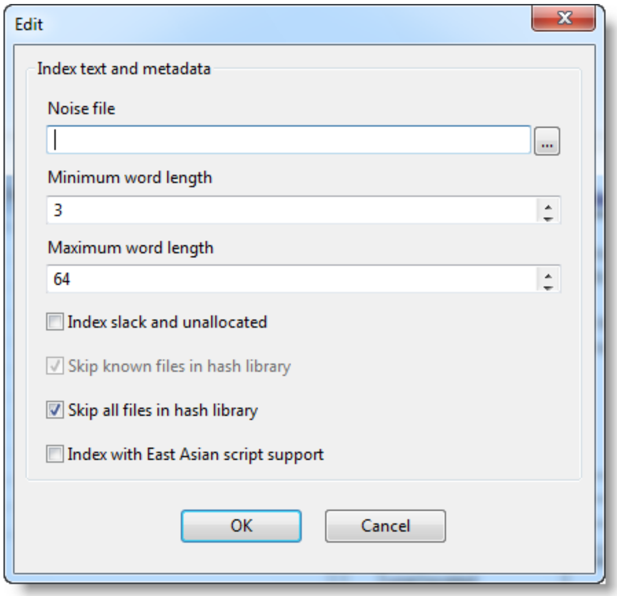
Choose this selection to create a searchable index of the data in the case. Creating an index will allow you to instantly search for terms in a variety of ways. You can adjust parameters for index creation, such as the minimum word length to index or whether to use a *noise file* (a file containing specific words to ignore).

Compared to keyword searches that search on the raw text, index searches will search on the transcript output of the file, which is critical for Microsoft Office 2007 and 2010 files.

Generating an index can take time, however, the trade-off in time spent creating the index yields a greater payoff with near instantaneous search times. Guidance Software, Inc. recommends always indexing your case data.

EnCase supports indexing text in slack bytes and unallocated space. As you select options for indexing within the Evidence Processor, you can choose to include text identified in file slack and unallocated space, defined below. This increases the total time for indexing text, but you could find the value of the indexed text to be worth the investment of time and resources.

- **File slack** – The area between the end of a file and the end of the last cluster or sector used by that file.
- **Unallocated space** – The sectors that are not associated with an allocated file—the free space of a disk or volume.



Edit

Index text and metadata

Noise file:

Minimum word length: 3

Maximum word length: 64

□ Index slack and unallocated

☑ Skip known files in hash library

☑ Skip all files in hash library

□ Index with East Asian script support

Figure 5-25 Index text and metadata

Unallocated space consists of either unwritten-to sectors or previously written-to sectors that no longer have historical attribution data associated with them. All these sectors are aggregated into Unallocated Clusters. Unallocated Clusters are then divided into multiple sections, and these sections are indexed with shared metadata. If a word at the end of one section of text spans to another section of text, that word is skipped and not included in the indexed sections of text.

The Evidence Processor uses identification processes to identify and differentiate ASCII, UTF-8/16/32 encodings as well as a number of East Asian and western codepages. The Evidence Processor uses built-in intelligence to index any text residing in slack and unallocated space.

NOTE: Indexing with East Asian script support is recommended, especially when Index Slack and Unallocated is enabled. The additional processing enabled by this option prevents meaningless strings that are otherwise identified as Unicode strings with Asian characters from being added to the index.

Sectors that are not assigned to any partition scheme fall under Unused Disk Area. The Evidence Processor handles these sectors and Unallocated Clusters similarly.

The following procedure provides the steps for including slack bytes and unallocated space when indexing text.

After you have selected the evidence you want to acquire and process with the Evidence Processor, select the Index text checkbox and click **Index text**. The Edit Settings dialog displays.

1. If you want to use a noise file, specify or browse to the filepath of your noise file
2. Set the minimum word length (1-128 characters) for indexed text
3. Select the checkbox for index slack and unallocated
4. If you want to index only the slack area of either known items or all items in the hash library, select the corresponding checkbox
5. To index using East Asian script support, select the corresponding checkbox
6. Click **OK**

Personal Information

- **Credit Cards** – Search document, database, and Internet files as categorized by the EnCase® File Types for the following credit card number formats: Visa, MasterCard, American Express, and Discover
    - Utilizes credit-card industry algorithms to validate the credit card number with about 90% accuracy
- **Phone Numbers** – Search document, database, and Internet files as categorized by the EnCase File Types for phone numbers with and/or without the area code
- **Email** – Search document, database, and Internet files as categorized by the EnCase File Types for e-mail addresses
- **Social Security Numbers** – Search document, database, and Internet files as categorized by the EnCase File Types for nine-digit United States Social Security numbers

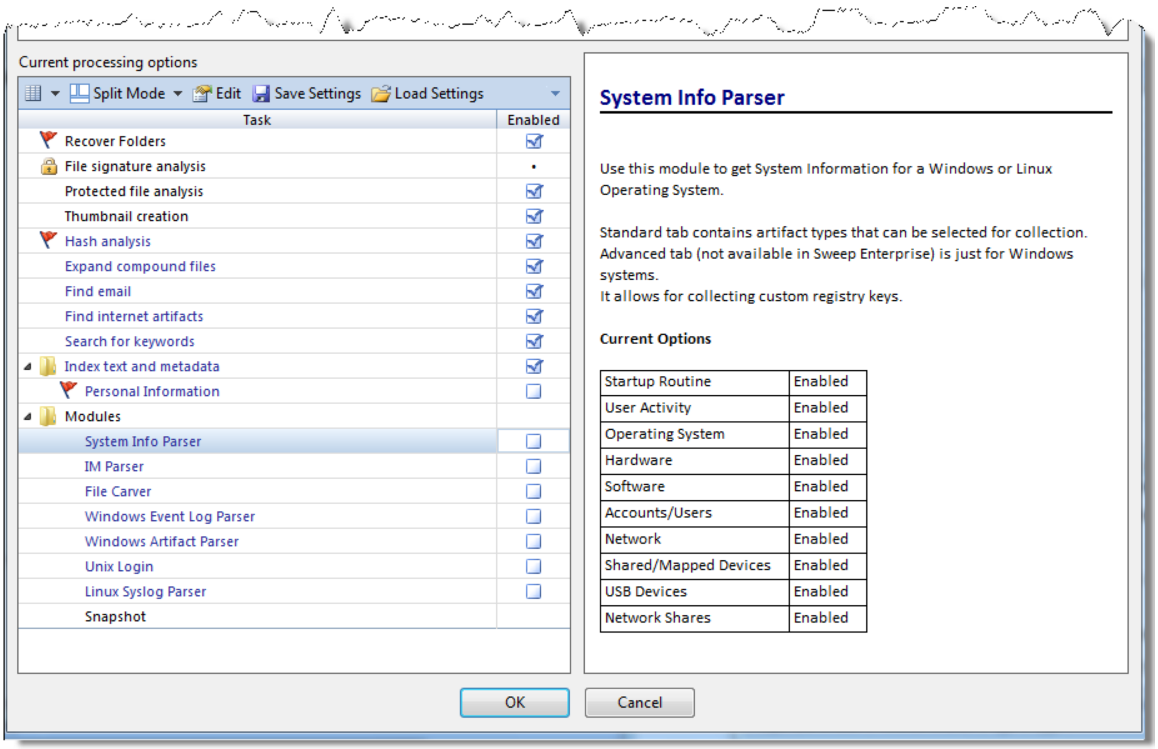
MODULES

The Evidence Processor has the ability to run add-in modules during processing. Some modules will ship as part of EnCase v7 and you can add your own modules as well. Click on the **Modules** folder to open it and access additional evidence processing features.

You should select the modules that are relevant to your case. The modules will add additional time to your processing, depending on the size of the evidence and the type of module selected as well as the module settings. Searching the unallocated clusters for evidence fragments, for example, will increase the processing time.

NOTE: *As best practice, you should not enable all modules by default. We will outline the essential function of each module.*

Click on the hyperlinked name of the module to configure the settings.



Current processing options

Task	Enabled
Recover Folders	☑
File signature analysis	•
Protected file analysis	☑
Thumbnail creation	☑
Hash analysis	☑
Expand compound files	☑
Find email	☑
Find internet artifacts	☑
Search for keywords	☑
Index text and metadata	☑
Personal Information	□
Modules	
System Info Parser	□
IM Parser	□
File Carver	□
Windows Event Log Parser	□
Windows Artifact Parser	□
Unix Login	□
Linux Syslog Parser	□
Snapshot	

System Info Parser

Use this module to get System Information for a Windows or Linux Operating System.

Standard tab contains artifact types that can be selected for collection.
Advanced tab (not available in Sweep Enterprise) is just for Windows systems.
It allows for collecting custom registry keys.

Current Options

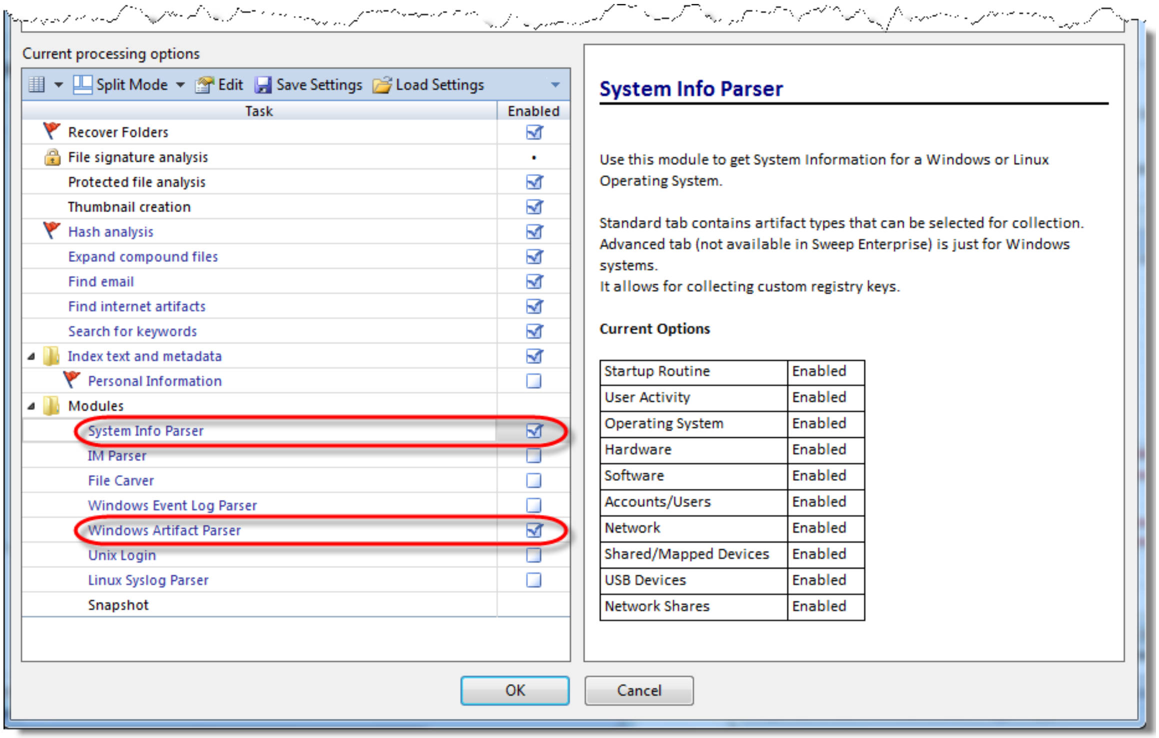
Startup Routine	Enabled
User Activity	Enabled
Operating System	Enabled
Hardware	Enabled
Software	Enabled
Accounts/Users	Enabled
Network	Enabled
Shared/Mapped Devices	Enabled
USB Devices	Enabled
Network Shares	Enabled

Figure 5-26 Evidence Processor Modules

- **System Info Parser** – Report on the core system information for Linux and Windows, including:
    - Startup routine (Linux only)
    - User activity (Linux only)
    - Operating system
    - Hardware
    - Software
    - Accounts/users
    - Network information
    - Shared/mapped drives
    - USB Devices
    - Network Shares
    - Advanced : Windows Registry
        - Time zone setting
        - Auto start
        - Hardware
        - User activity
        - User defined keys
        - Networking and other autorun
            - When you select the **System Info** option in the Evidence Processor, you can search **NetShare** and **USB** registry information in the Records tab. You can see the UNC path visit history, the history of connected devices, and you can correlate USB devices to their drive letters.
- **IM Parser** – Search for Instant Messenger artifacts from MSN®, Yahoo®, and AOL Instant Messenger clients. These artifacts include messages and buddy-list contents. It also allows you to select where to search from several general location categories.
    - All or selected files, and/or Unallocated Clusters
- **File Carver** – Search evidence for file fragments based on a specific set of parameters, such as known file size and file
    - The EnCase File Carver function automatically checks file headers for file length information and uses the actual number of bytes carved, by default. This produces more accurate carved files. When there is no file length information in the header, the footer or the default length is used. This additional parsing is not user configurable.
    - Search all or selected files, file slack, and/or unallocated clusters for deleted or embedded files by header

  - Over 300 file types are supported for carving, including carving HTML files and webmail by keywords
  - Running the File Carver in Evidence Processor gives you three options; you can select from either the full file types table, from the optimized file types table, or from both. Optimized file types include:
    - Compound document file
    - Outlook personal folder
    - Audio Video Interleave
    - Flash video files
    - Enhanced Metafile Graphic
    - Microsoft bitmap format
  - When the File Carver finishes, you can see the files carved and optionally export the files for review.
- **Windows Event Log Parser** – Locate and parse Windows Event Logs
  - Parse EVT and EVTX files, including filtering by type of event
- **Windows Artifact Parser** – Report on Windows artifacts, including
  - Link files
  - Recycle Bin files
  - MFT (NTFS Master File Table) transactions
  - All or selected files, and/or unallocated clusters
- **Unix Login** – Search UNIX log files for specific events
- **Linux Syslog Parser** – Search Linux syslog files for specific events
- **Snapshot** – (Live preview of devices only) – Running processes, open ports, logged on users, etc.

For now, select **System Info Parser** and **Windows Artifacts Parser**.



Current processing options

Task	Enabled
Recover Folders	☑
File signature analysis	•
Protected file analysis	☑
Thumbnail creation	☑
Hash analysis	☑
Expand compound files	☑
Find email	☑
Find internet artifacts	☑
Search for keywords	☑
Index text and metadata	☑
Personal Information	□
Modules	
System Info Parser	☑
IM Parser	□
File Carver	□
Windows Event Log Parser	□
Windows Artifact Parser	☑
Unix Login	□
Linux Syslog Parser	□
Snapshot	

System Info Parser

Use this module to get System Information for a Windows or Linux Operating System.

Standard tab contains artifact types that can be selected for collection.
Advanced tab (not available in Sweep Enterprise) is just for Windows systems.
It allows for collecting custom registry keys.

Current Options

Startup Routine	Enabled
User Activity	Enabled
Operating System	Enabled
Hardware	Enabled
Software	Enabled
Accounts/Users	Enabled
Network	Enabled
Shared/Mapped Devices	Enabled
USB Devices	Enabled
Network Shares	Enabled

Figure 5-27 EnCase Evidence Processor

After finishing the EnCase Evidence Processor configuration, click **OK**. The time acquired to complete the processing depends on the size of evidence and the processing options selected. More processing power, RAM, disk I/O, etc., will affect the speed.

NOTE: With the options selected in the example, it will take several hours to fully process the evidence dependent upon your machine's processor, RAM, hard drives, etc. However you can continue to browse, examine, and bookmark the evidence as you would with prior versions of EnCase.

You will see the Evidence Processor running in the lower right corner and you can continue your analysis of the evidence when it processes.

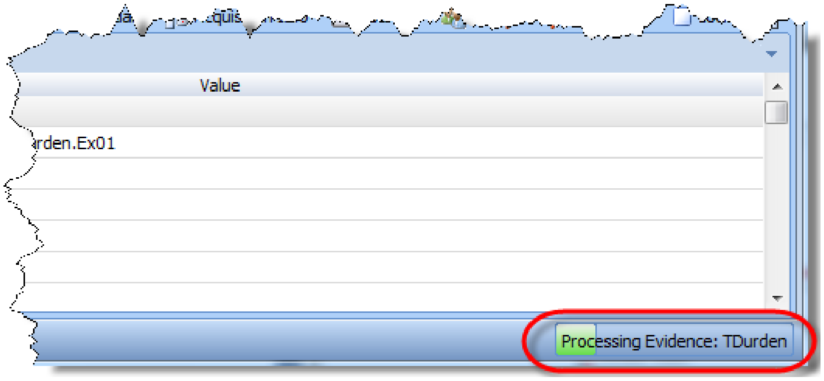


Figure 5-28 EnCase Evidence Processor running

As the modules are processed, you will see the status change.

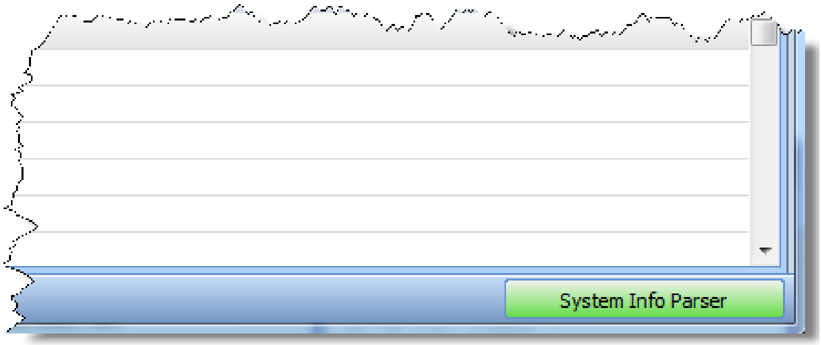


Figure 5-29 EnCase Evidence Processor running – Modules

Processing a Live Device

The EnCase Evidence Processor also can process live devices. This allows you to bypass acquiring evidence before and directly process the evidence. All options are available for all processing except for Index text. The following procedure provides the steps for processing devices from a device preview.

From the Home tab of an open case, click **Add Evidence**. The Add Evidence screen displays.

Click **Add Local Device…** or **Add Crossover Preview…** The Add Device dialog displays.

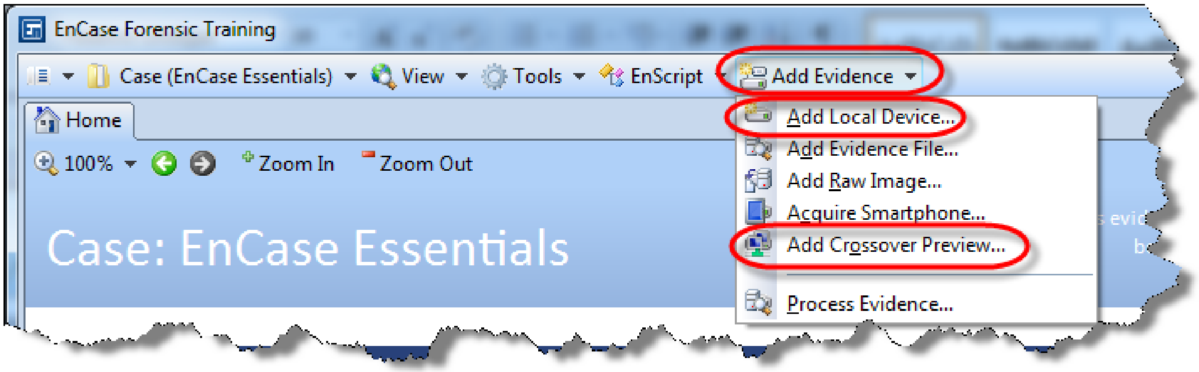


Figure 5-30 Add live device

1. Select the checkboxes of the devices you want to add to the preview and click **Finish**
   - The Evidence tab displays with a preview of the chosen devices
2. In the Evidence tab, click **Process Evidence**
   - The Evidence Processor dialog displays.
3. Under Process, select the checkboxes for the live devices you want to process
4. Review and, if necessary, modify the current processing options
5. Click **OK**

Evidence Processor Threading Model

The EnCase Evidence Processor has improved threading capabilities. Please see the diagram for more detail.

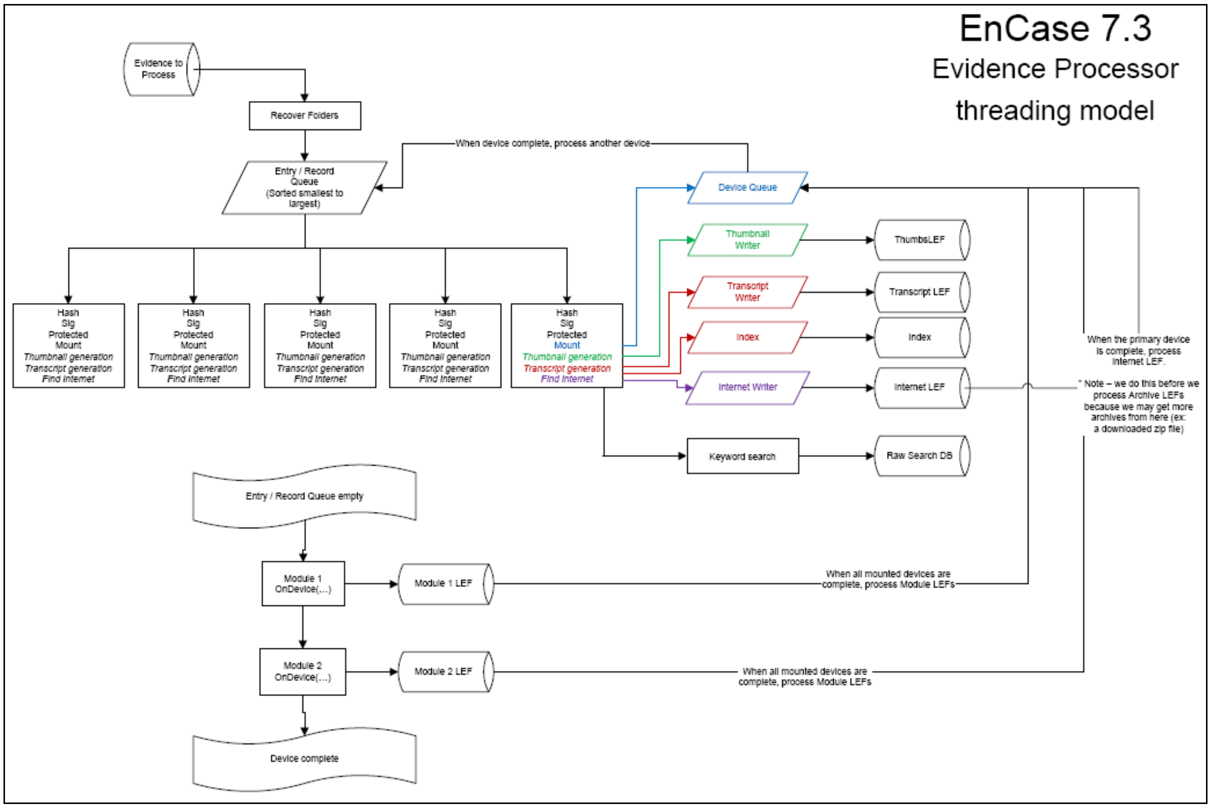
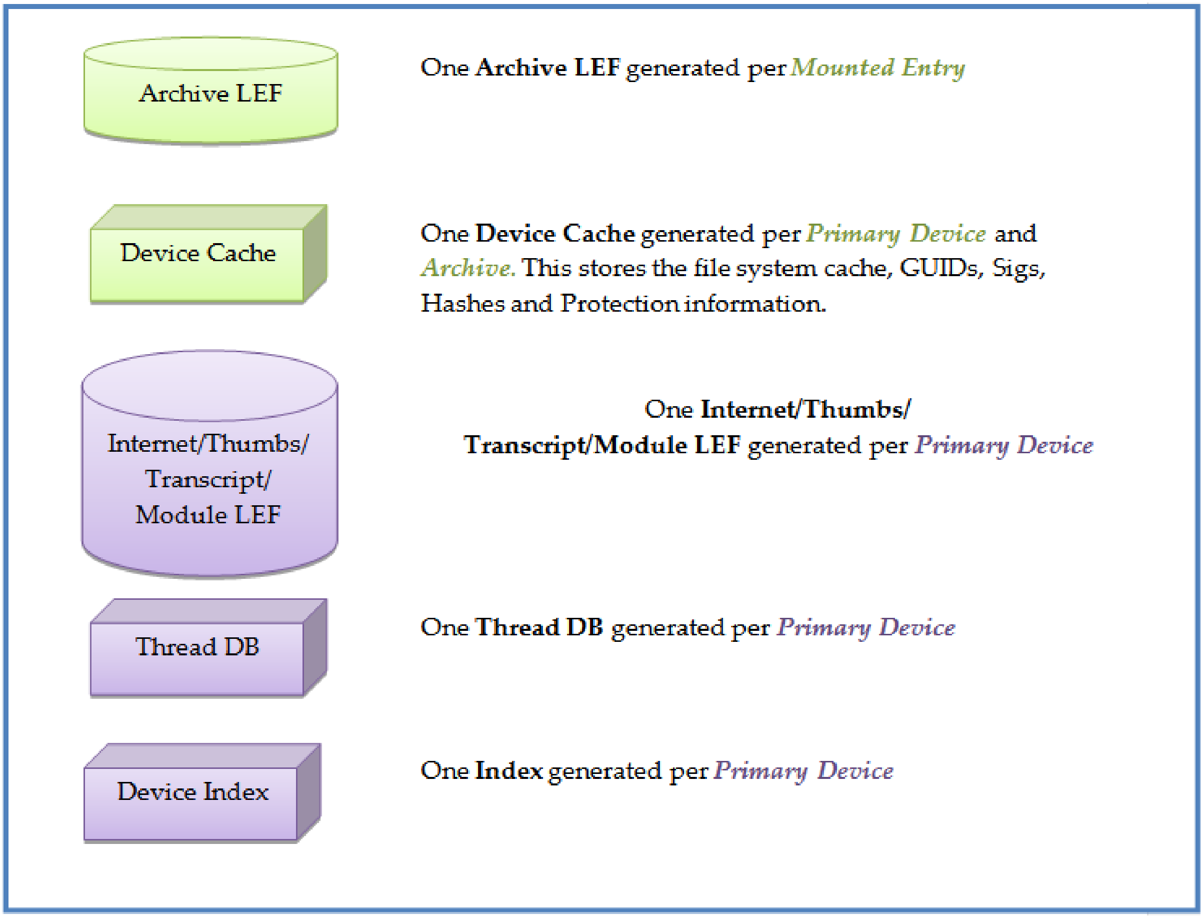

EnCase 7.3
Evidence Processor
threading model
Evidence to Process
Recover Folders
When device complete, process another device
Entry / Record Queue (Sorted smallest to largest)
Hash Sig Protected Mount Thumbnail generation Transcript generation Find Internet
Hash Sig Protected Mount Thumbnail generation Transcript generation Find Internet
Hash Sig Protected Mount Thumbnail generation Transcript generation Find Internet
Hash Sig Protected Mount Thumbnail generation Transcript generation Find Internet
Hash Sig Protected Mount Thumbnail generation Transcript generation Find Internet
Device Queue
Thumbnail Writer
Transcript Writer
Index
Internet Writer
Keyword search
ThumbsLEF
Transcript LEF
Index
Internet LEF
Raw Search DB
When the primary device is complete, process Internet LEF.
* Note – we do this before we process Archive LEFs because we may get more archives from here (ex: a downloaded zip file)
Entry / Record Queue empty
Module 1 OnDevice(…)
Module 1 LEF
When all mounted devices are complete, process Module LEFs
Module 2 OnDevice(…)
Module 2 LEF
When all mounted devices are complete, process Module LEFs
Device complete

Figure 5-31 EnCase Evidence Processor threading model



One **Archive LEF** generated per *Mounted Entry*

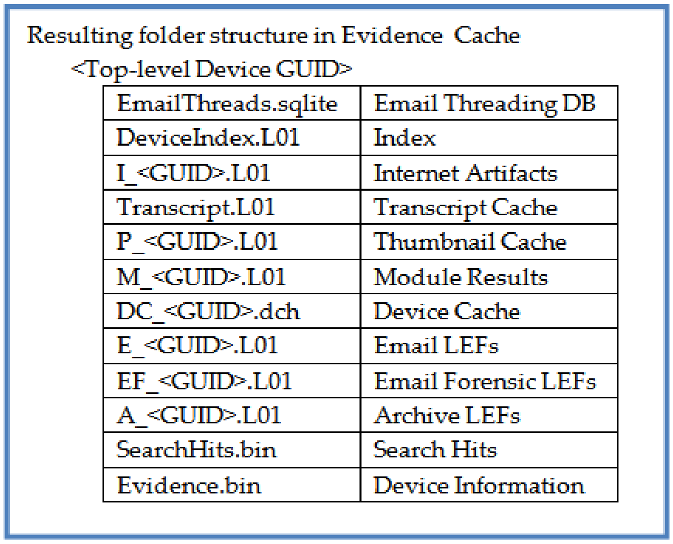
One **Device Cache** generated per *Primary Device* and *Archive.* This stores the file system cache, GUIDs, Sigs, Hashes and Protection information.

One **Internet/Thumbs/ Transcript/Module LEF** generated per *Primary Device*

One **Thread DB** generated per *Primary Device*

One **Index** generated per *Primary Device*

Figure 5-32 EnCase Evidence Processor – evidence cache and index



Resulting folder structure in Evidence Cache

<Top-level Device GUID>

EmailThreads.sqlite	Email Threading DB
DeviceIndex.L01	Index
I_<GUID>.L01	Internet Artifacts
Transcript.L01	Transcript Cache
P_<GUID>.L01	Thumbnail Cache
M_<GUID>.L01	Module Results
DC_<GUID>.dch	Device Cache
E_<GUID>.L01	Email LEFs
EF_<GUID>.L01	Email Forensic LEFs
A_<GUID>.L01	Archive LEFs
SearchHits.bin	Search Hits
Evidence.bin	Device Information

Figure 5-33 Evidence Cache folder structure

Notes

Notes

Notes

Lesson 6

Viewing Index and Search Results

EnCase® v7 provides core enhancements to searching, such as:

- The ability to search across multiple types of data, including files, e-mail, and Internet history, as well as view the results on a single screen
- A powerful index search capability
- The ability to search based on user-customized tags

Search Types

There are three principal methods of searching through evidence in EnCase v7:

- **Index searches** – Evidence data is indexed through the EnCase® Evidence Processor prior to searching
- **Raw searches** – Searches based on non-indexed, raw data
- **Tag searches** – Searches based on user-defined tags

Index Searches

Using the Evidence Processor, you create an index, a list of words from the contents of a device. The index entries contain pointers to the occurrences of the specific word on the device.

There are two steps to using indexes:

- Generating an index (covered in the previous *Processing Evidence Files* lesson)
- Searching an index

Generating an index creates index files associated with devices. Creating an index can be time consuming, depending on the amount of evidence you are indexing as well as the capabilities of your computer hardware. Evidence file size, and thus the resultant index size, is an important consideration when building an index. Attempts to index extremely large evidence files can tax a computer's resources.

You generate a search index early in the EnCase v7 workflow sequence as follows:

- Make sure that your case contains the device you want to index
- As you may recall from a prior lesson, click **Process Evidence** from the Evidence menu
  - o The Evidence Processor displays; this dialog contains the selection for indexing text
- Follow the instructions detailed in the Processing Evidence Files lesson

During the creation of an index, the transcript text of the file is extracted using Outside In technology, and then the text is broken into words that are added to the index. Unlike raw keyword searches, indexing is done against the transcript content of the file so that text contained in compound files, such as Microsoft Office 2007 and 2010 files, can be properly identified. Although EnCase v7 does not create a transcript of slack space and unallocated space, they are processed and broken into words in the best manner possible so that EnCase v7 can find hits in those areas also.

Index searching (queries) allows you to rapidly search for terms in the generated index and it is the recommended type of search in EnCase v7.

Creating a Search Query

Once your case has been indexed, keyword searched, tagged, or any combination of the three, you can then search for desired information. To create a unified search do the following:

1. Go to the **Home** screen and click the **Search** button.

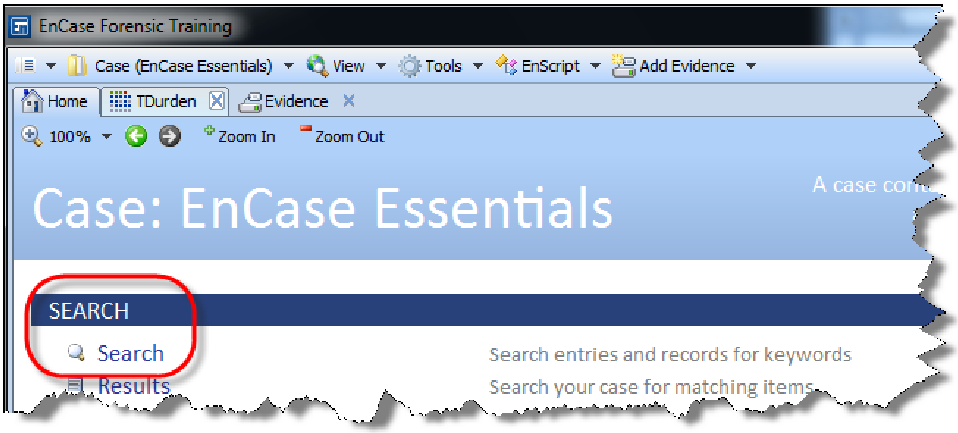
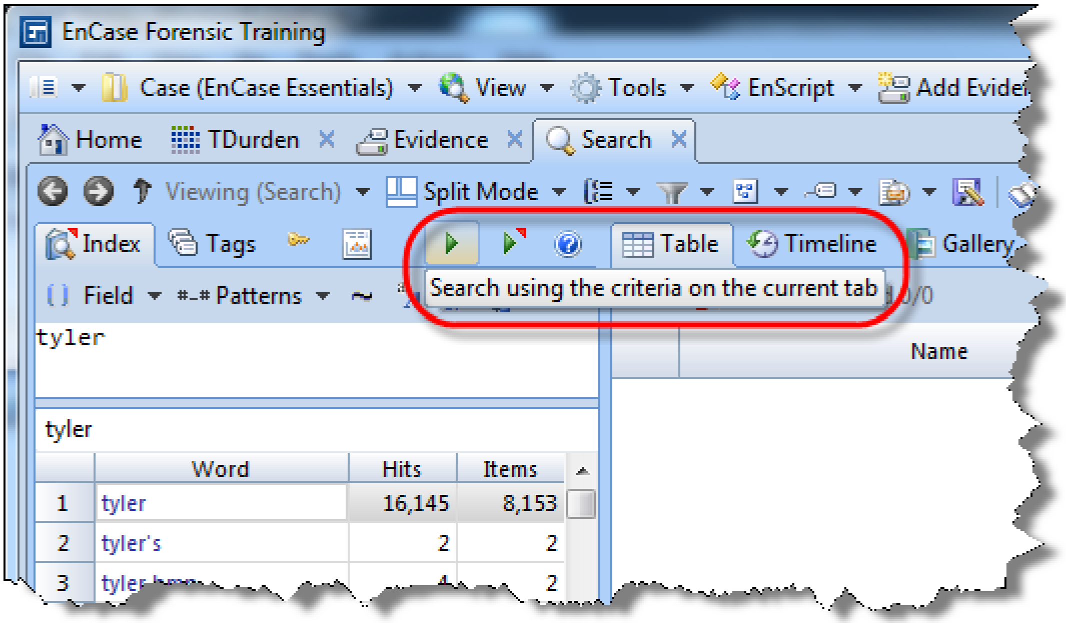


Figure 6-1 New Search…

2. In the Index window, enter the keyword(s) to query the Index, such as "Tyler."
3. A dynamic list is displayed on the right side of the window, showing the terms in the index and the number of occurrence of a term. This is extremely helpful when crafting a query so that you can immediately see if the term exists in the index.

4. EnCase v7 will show you all words in the index that start with the term that you have typed and will dynamically update the list as you type additional letters. At any time you can double-click on a query term and it will show the show the information about that term

5. Click on the **Play** button to run the query.



Search using the criteria on the current tab

tyler

tyler

	Word	Hits	Items
1	tyler	16,145	8,153
2	tyler's	2	2
3	tyler	4	2

Figure 6-2 New Search interface

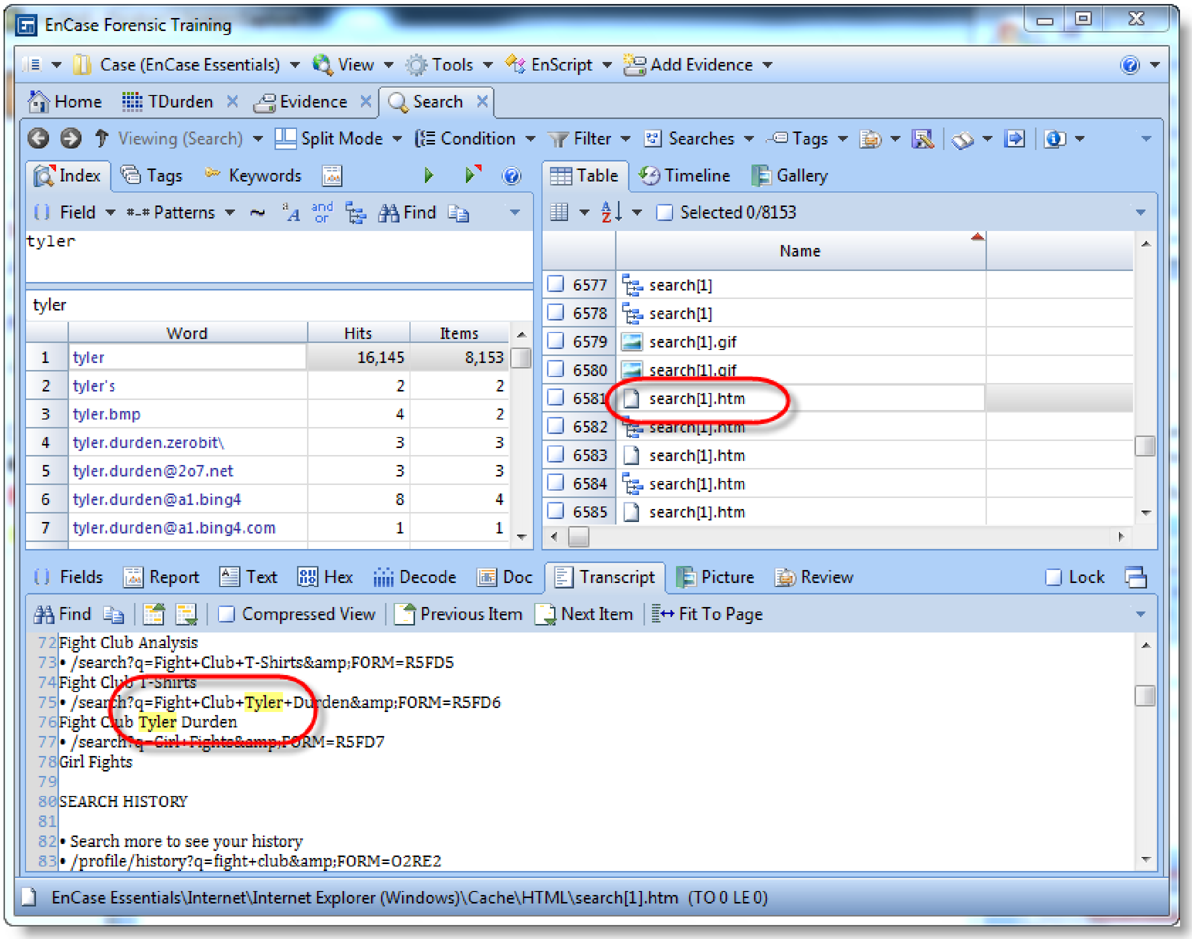
For examples of index query options, see the *Appendix A – Index Queries* at the end of this manual.

EnCase v7 will run the query display the results in the Table Pane of the Search view.

You can review the file entries that contain the search term; for example, the webpage `search[1].htm` displays as follows.

The Index query hits are displayed in yellow in the Transcript tab of the View Pane. Use the **Next Hit** button to view the search hit in a large file.

NOTE: Raw Keyword search hits can be viewed in the Text tab.



tyler

tyler

	Word	Hits	Items
1	tyler	16,145	8,153
2	tyler's	2	2
3	tyler.bmp	4	2
4	tyler.durden.zerobit\	3	3
5	tyler.durden@2o7.net	3	3
6	tyler.durden@a1.bing4	8	4
7	tyler.durden@a1.bing4.com	1	1

	Name
6577	search[1]
6578	search[1]
6579	search[1].gif
6580	search[1].gif
6581	search[1].htm
6582	search[1].htm
6583	search[1].htm
6584	search[1].htm
6585	search[1].htm

```
Fight Club Analysis
• /search?q=Fight+Club+T-Shirts&amp;FORM=R5FD5
Fight Club T-Shirts
• /search?q=Fight+Club+Tyler+Durden&amp;FORM=R5FD6
Fight Club Tyler Durden
• /search?q=Girl+Fights&amp;FORM=R5FD7
Girl Fights

SEARCH HISTORY

• Search more to see your history
• /profile/history?q=fight+club&amp;FORM=O2RE2
```

EnCase Essentials\Internet\Internet Explorer (Windows)\Cache\HTML\search[1].htm (TO 0 LE 0)

Figure 6-3 Search result

Save the Search Results

You can save the results of the search for future quick access in the **Results** view.

Click on the **Searches** drop-down menu and select **Save As…**

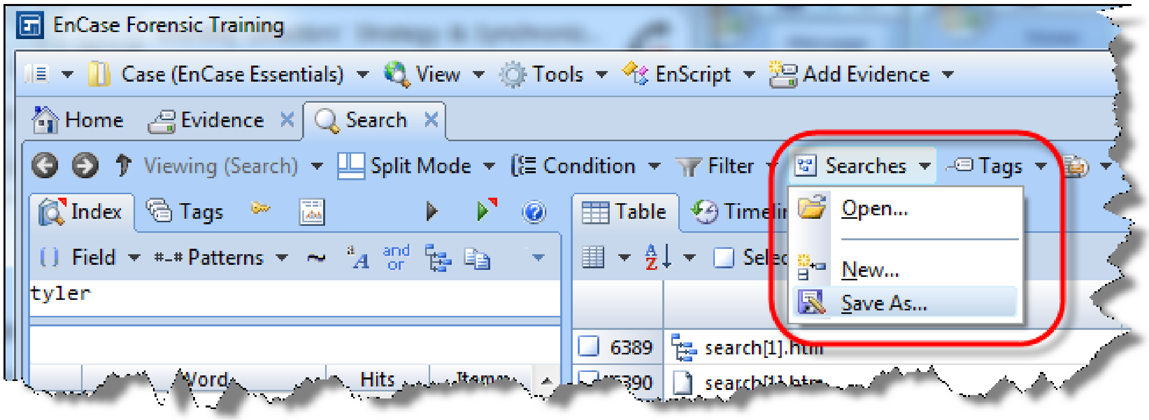
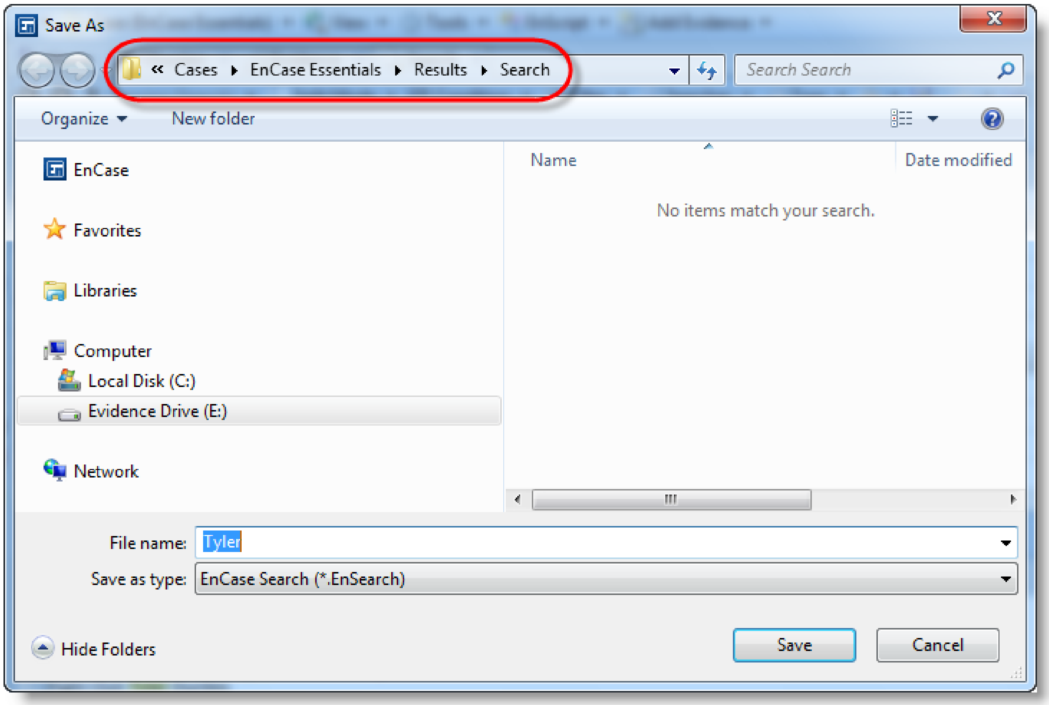


Figure 6-4 Save Search Result

The default location is the Search folder under your case.



File name: Tyler

Save as type: EnCase Search (*.EnSearch)

Figure 6-5 Saving search result

When appropriate, you can switch over to the **Results** tab to view the saved results.

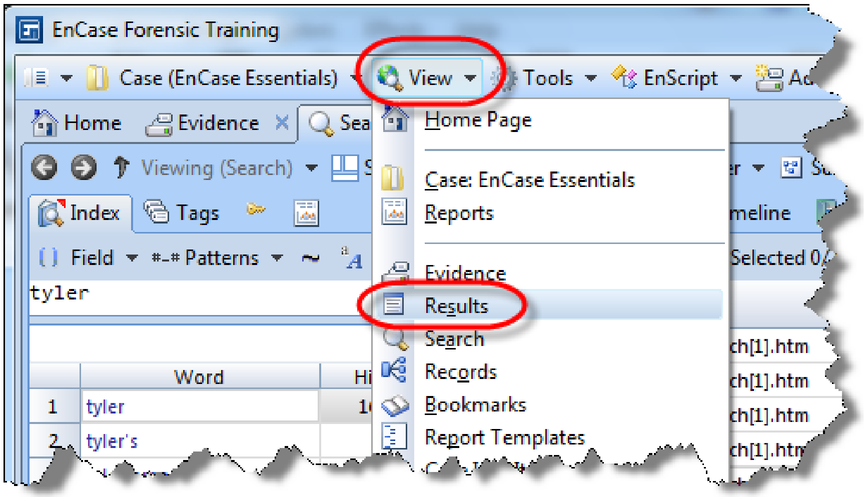
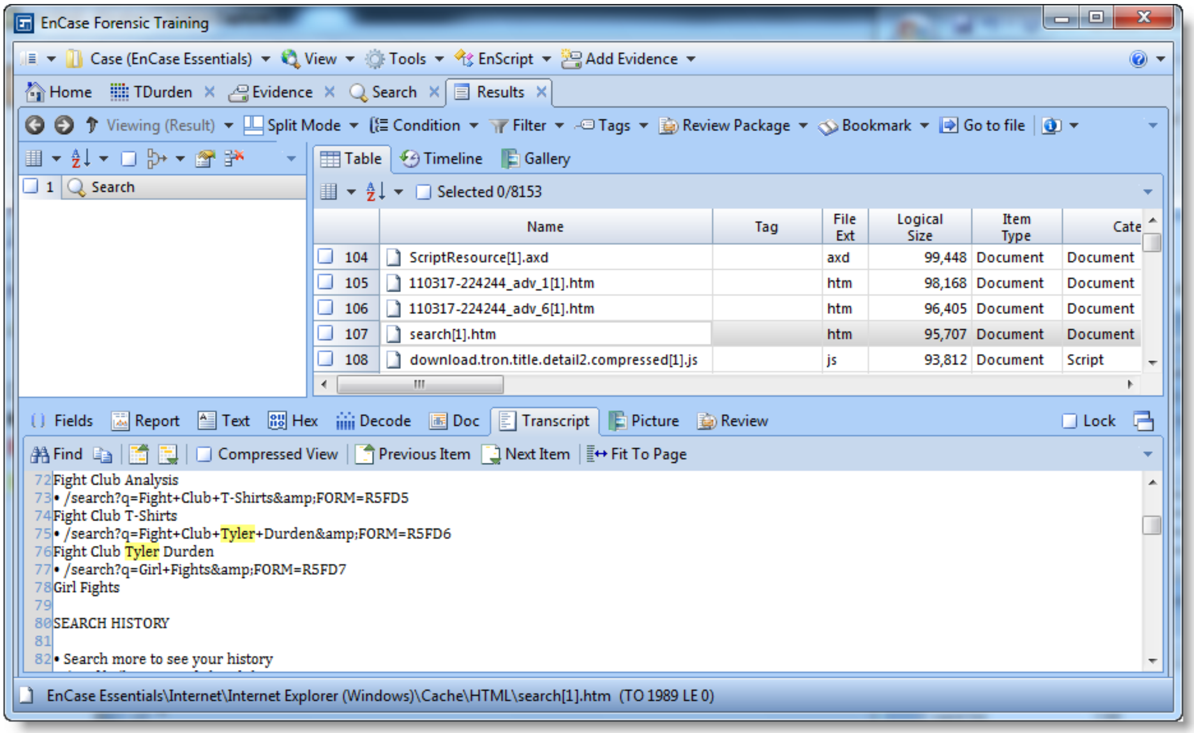


Figure 6-6 Results tab

The saved search is available for analysis.



Selected 0/8153

	Name	Tag	File Ext	Logical Size	Item Type	Cate
104	ScriptResource[1].axd		axd	99,448	Document	Document
105	110317-224244_adv_1[1].htm		htm	98,168	Document	Document
106	110317-224244_adv_6[1].htm		htm	96,405	Document	Document
107	search[1].htm		htm	95,707	Document	Document
108	download.tron.title.detail2.compressed[1].js		js	93,812	Document	Script

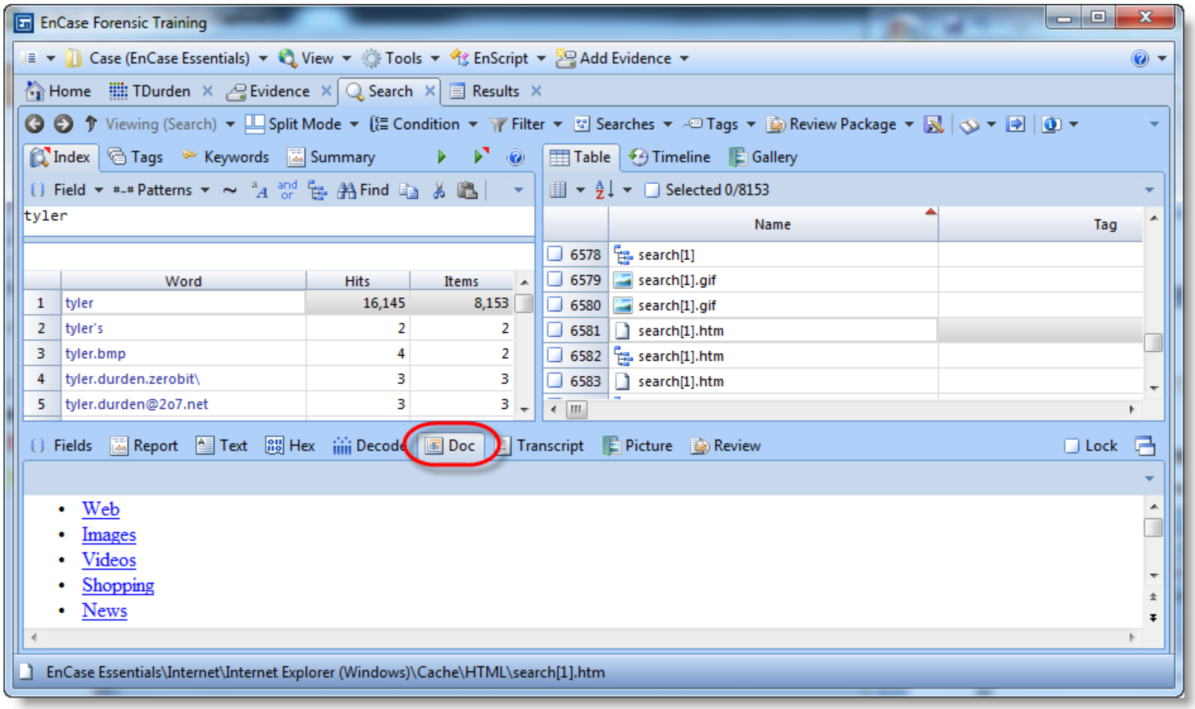
```
Fight Club Analysis
• /search?q=Fight+Club+T-Shirts&amp;FORM=R5FD5
Fight Club T-Shirts
• /search?q=Fight+Club+Tyler+Durden&amp;FORM=R5FD6
Fight Club Tyler Durden
• /search?q=Girl+Fights&amp;FORM=R5FD7
Girl Fights

SEARCH HISTORY

• Search more to see your history
```

EnCase Essentials\Internet\Internet Explorer (Windows)\Cache\HTML\search[1].htm (TO 1989 LE 0)

Figure 6-7 Results tab – saved search

Continue the Investigation

Returning to the Search view, you can switch over to the **Doc** view to see the webpage in HTML.


EnCase Forensic Training
Case (EnCase Essentials) View Tools EnScript Add Evidence
Home TDurden Evidence Search Results
Viewing (Search) Split Mode Condition Filter Searches Tags Review Package
Index Tags Keywords Summary
Table Timeline Gallery
Field Patterns Find
Selected 0/8153
Fields Report Text Hex Decode Doc Transcript Picture Review Lock

tyler

	Word	Hits	Items
1	tyler	16,145	8,153
2	tyler's	2	2
3	tyler.bmp	4	2
4	tyler.durden.zerobit\	3	3
5	tyler.durden@2o7.net	3	3

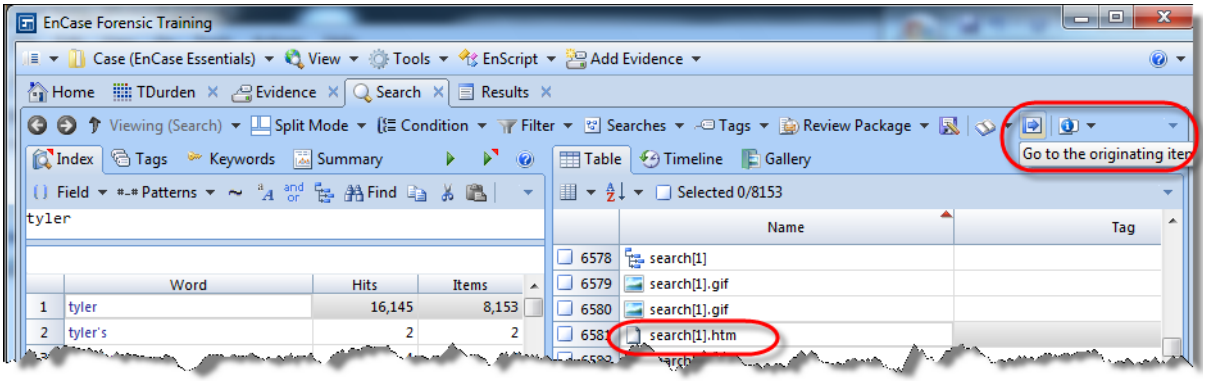
	Name	Tag
6578	search[1]	
6579	search[1].gif	
6580	search[1].gif	
6581	search[1].htm	
6582	search[1].htm	
6583	search[1].htm	

- Web
- Images
- Videos
- Shopping
- News

EnCase Essentials\Internet\Internet Explorer (Windows)\Cache\HTML\search[1].htm

Figure 6-8 Doc view

To see the file in the context of the evidence, click on **Go to file**.


EnCase Forensic Training
Case (EnCase Essentials) View Tools EnScript Add Evidence
Home TDurden Evidence Search Results
Viewing (Search) Split Mode Condition Filter Searches Tags Review Package
Go to the originating iter
Index Tags Keywords Summary
Table Timeline Gallery
Field Patterns Find
Selected 0/8153

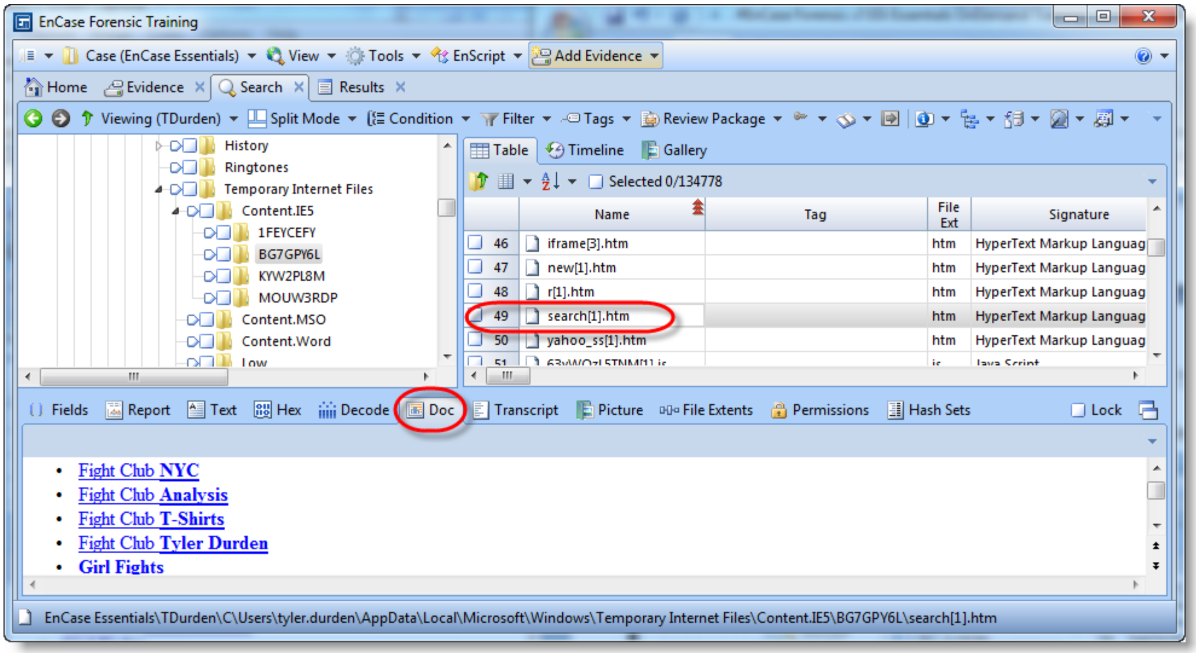
tyler

	Word	Hits	Items
1	tyler	16,145	8,153
2	tyler's	2	2

	Name	Tag
6578	search[1]	
6579	search[1].gif	
6580	search[1].gif	
6581	search[1].htm	

Figure 6-9 Go to file

You will be taken to the Entries view of the Search Results tab to analyze the evidence in context.



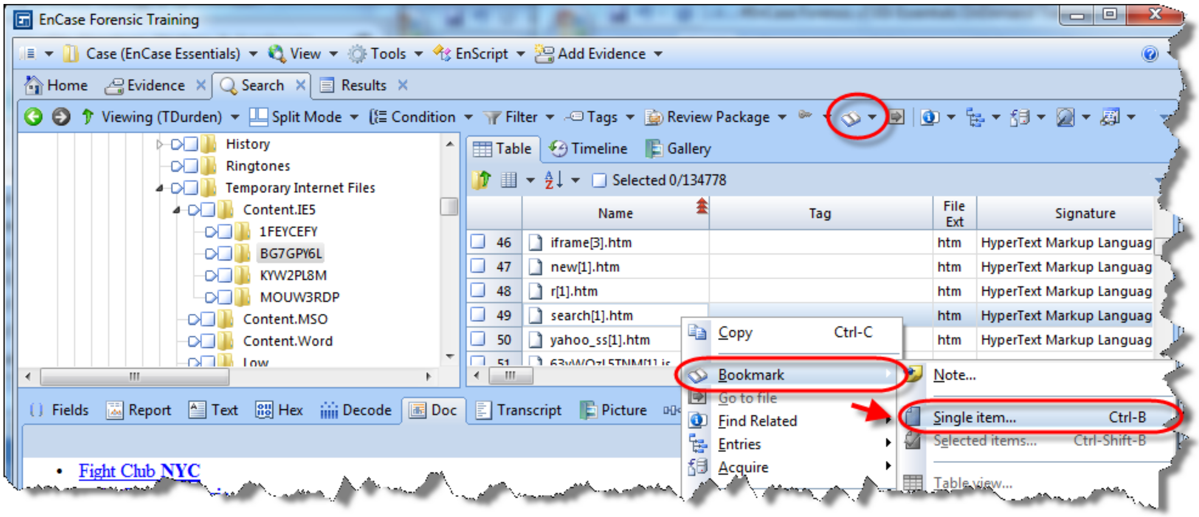
	Name	Tag	File Ext	Signature
46	iframe[3].htm		htm	HyperText Markup Languag
47	new[1].htm		htm	HyperText Markup Languag
48	r[1].htm		htm	HyperText Markup Languag
49	search[1].htm		htm	HyperText Markup Languag
50	yahoo_ss[1].htm		htm	HyperText Markup Languag
51	63vWOzI5TNM[1].js		js	Java Script

- Fight Club NYC
- Fight Club Analysis
- Fight Club T-Shirts
- Fight Club Tyler Durden
- Girl Fights

EnCase Essentials\TDurden\C\Users\tyler.durden\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\BG7GPY6L\search[1].htm

Figure 6-10 File in context of entries

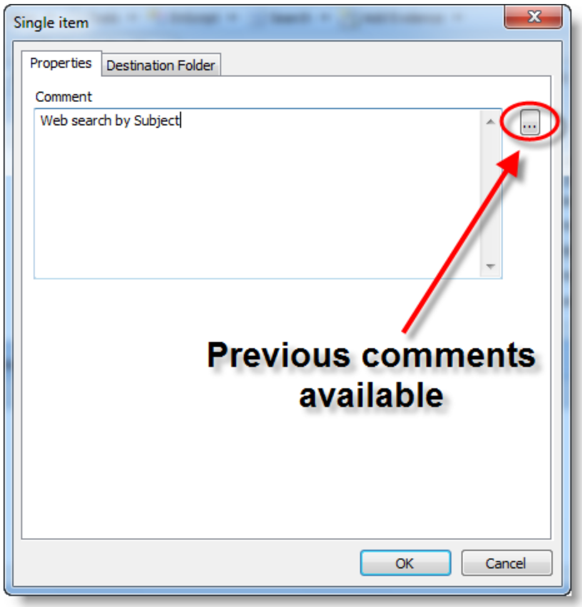
You can bookmark the evidence from either the Search, Results or the Evidence view.



	Name	Tag	File Ext	Signature
46	iframe[3].htm		htm	HyperText Markup Languag
47	new[1].htm		htm	HyperText Markup Languag
48	r[1].htm		htm	HyperText Markup Languag
49	search[1].htm		htm	HyperText Markup Languag
50	yahoo_ss[1].htm		htm	HyperText Markup Languag
51	63vWOzI5TNM[1].js			

Figure 6-11 Bookmark in Results view

You can add a comment to the bookmarked evidence and have the ability to use previous comments to save time.



Comment: Web search by Subject

Previous comments available

Figure 6-12 Bookmark comments

Choose the folder in the case template to add the evidence or create a new folder. It will default to the last-selected folder to save time, so you don't have to select the destination folder for each bookmark.

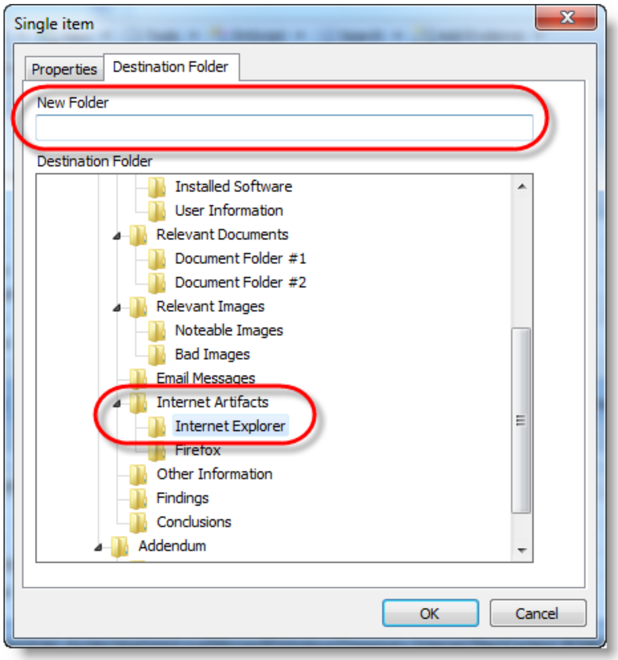


Figure 6-13 Bookmark Destination Folder

Use the **Back** button to return to the Search Results view of the query results.

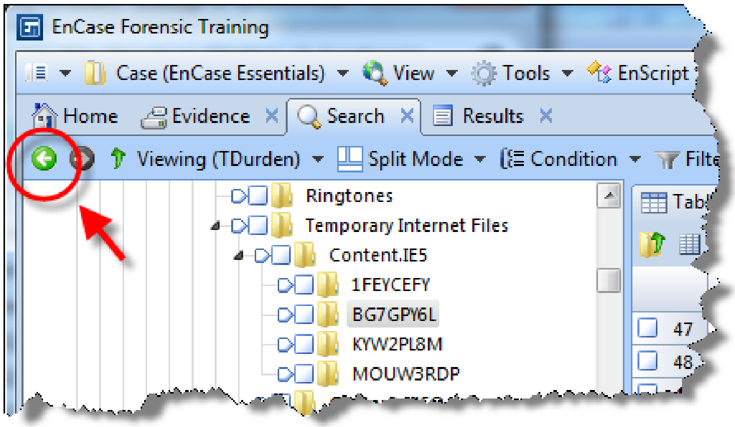
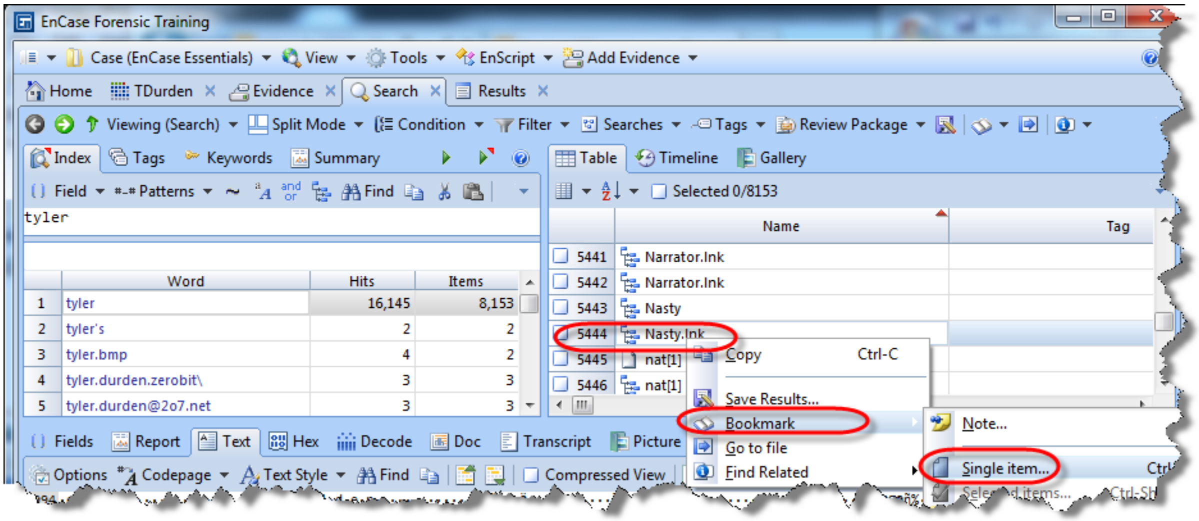


Figure 6-14 Back to Search Results query

Find Related

New to EnCase v7 is the **Find related** button, allowing you to find related files and folders by name or by time.

In this instance, in the Results view you found a link file called "Nasty.lnk," showing that the user knew the folder or file was on the computer system and made an affirmative act by manually opening the folder or file. This would be a good artifact to bookmark and investigative lead to follow.



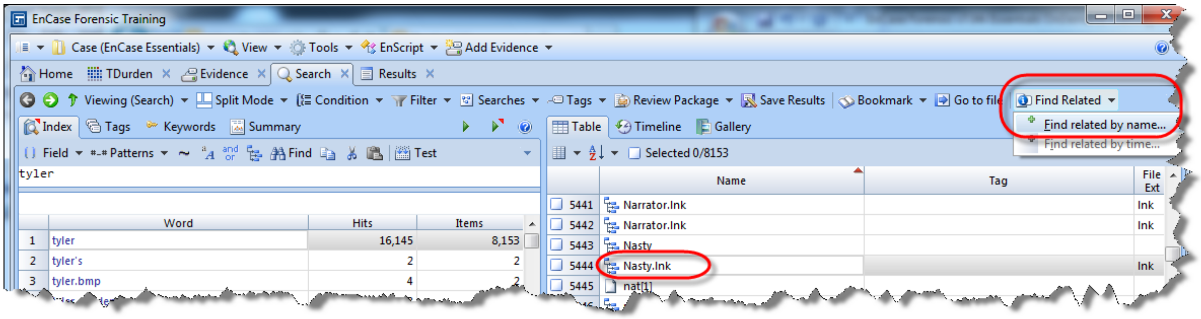
tyler

	Word	Hits	Items
1	tyler	16,145	8,153
2	tyler's	2	2
3	tyler.bmp	4	2
4	tyler.durden.zerobit\	3	3
5	tyler.durden@2o7.net	3	3

	Name	Tag
5441	Narrator.lnk	
5442	Narrator.lnk	
5443	Nasty	
5444	Nasty.lnk	
5445	nat[1]	
5446	nat[1]	

Figure 6-15 Bookmark the evidence

Click on **Find related by name...**.


EnCase Forensic Training
Case (EnCase Essentials) View Tools EnScript Add Evidence
Home TDurden Evidence Search Results
Viewing (Search) Split Mode Condition Filter Searches Tags Review Package Save Results Bookmark Go to file
Find Related
Find related by name...
Find related by time...
Index Tags Keywords Summary
Table Timeline Gallery
Field Patterns Find Test
Selected 0/8153

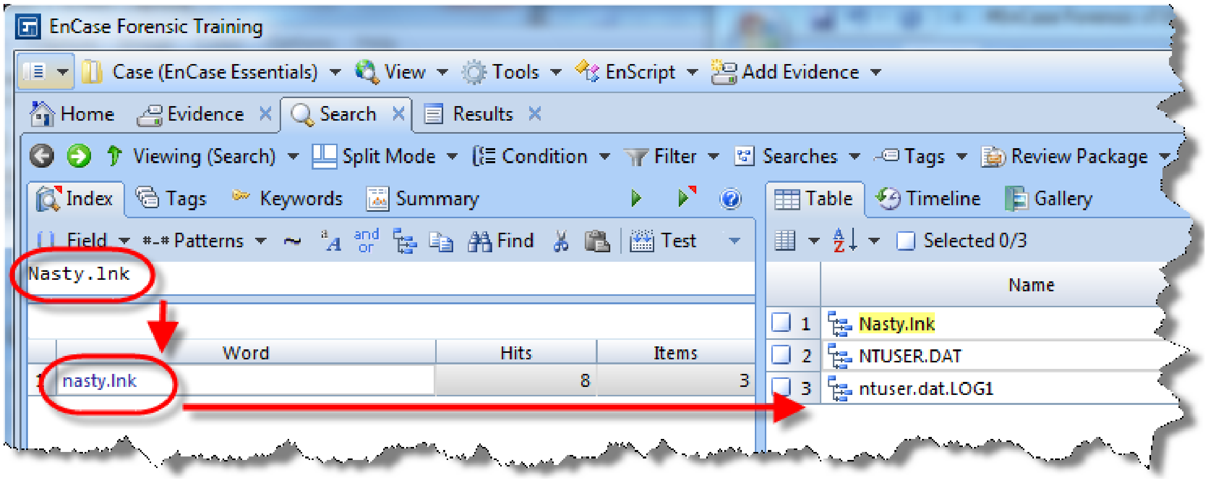
tyler

	Word	Hits	Items
1	tyler	16,145	8,153
2	tyler's	2	2
3	tyler.bmp	4	2

	Name	Tag	File Ext
5441	Narrator.lnk		lnk
5442	Narrator.lnk		lnk
5443	Nasty		
5444	Nasty.lnk		lnk
5445	nat[1]		

Figure 6-16 Find related by name...

The name will appear in a new Index query. Click on the hyperlink below the Index window to see the results in the Table Pane.


EnCase Forensic Training
Case (EnCase Essentials) View Tools EnScript Add Evidence
Home Evidence Search Results
Viewing (Search) Split Mode Condition Filter Searches Tags Review Package
Index Tags Keywords Summary
Table Timeline Gallery
Field Patterns Find Test
Selected 0/3

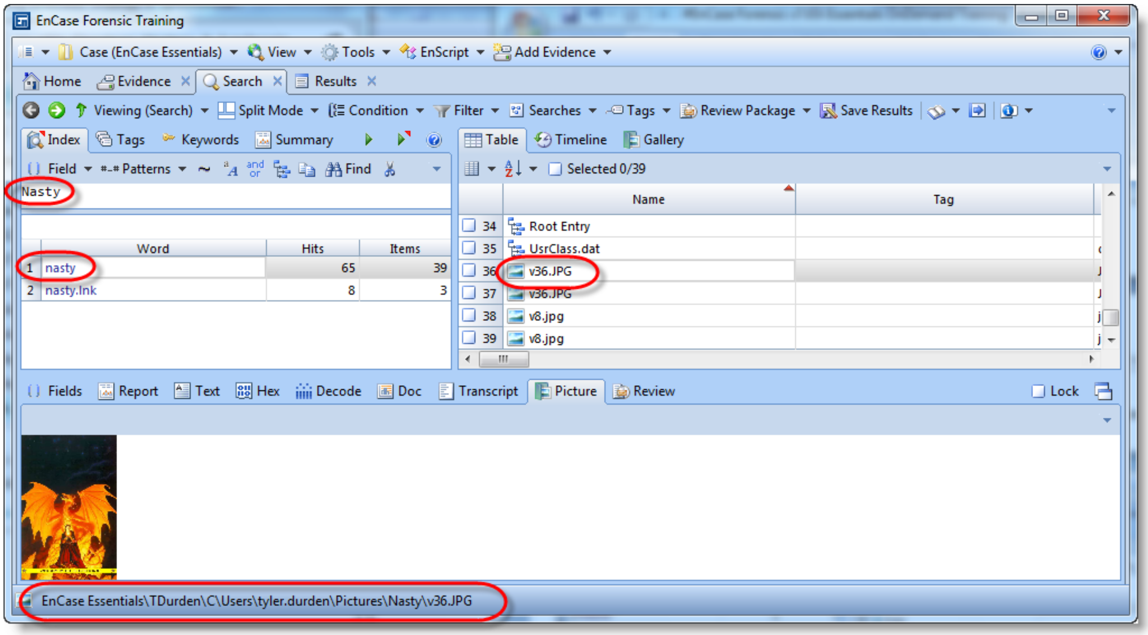
Nasty.lnk

	Word	Hits	Items
1	nasty.lnk	8	3

	Name
1	Nasty.lnk
2	NTUSER.DAT
3	ntuser.dat.LOG1

Figure 6-17 Index query

Shorten the text query to "Nasty" to see additional related items of evidence. Click on the hyperlink to see the results in the Table Pane.



Nasty

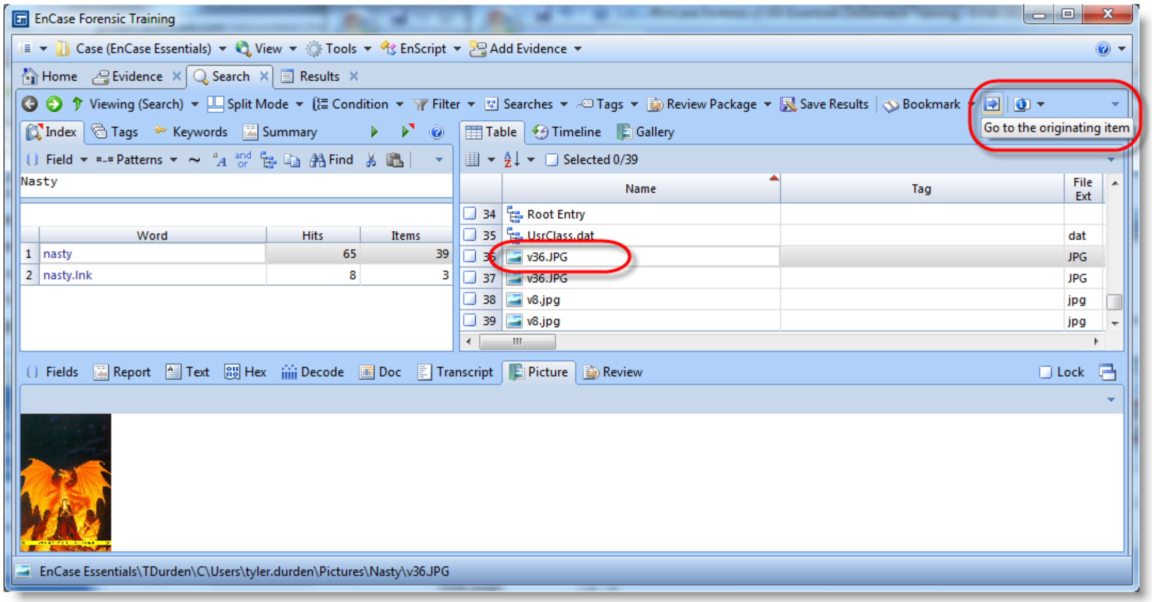
	Word	Hits	Items
1	nasty	65	39
2	nasty.lnk	8	3

	Name	Tag
34	Root Entry	
35	UsrClass.dat	
36	v36.JPG	
37	v36.JPG	
38	v8.jpg	
39	v8.jpg	

EnCase Essentials\TDurden\C\Users\tyler.durden\Pictures\Nasty\v36.JPG

Figure 6-18 Query for "Nasty"

When you find a file you wish to investigate further, use the **Go to file** button to view it in the context of the Evidence folder structure.



Nasty

	Word	Hits	Items
1	nasty	65	39
2	nasty.lnk	8	3

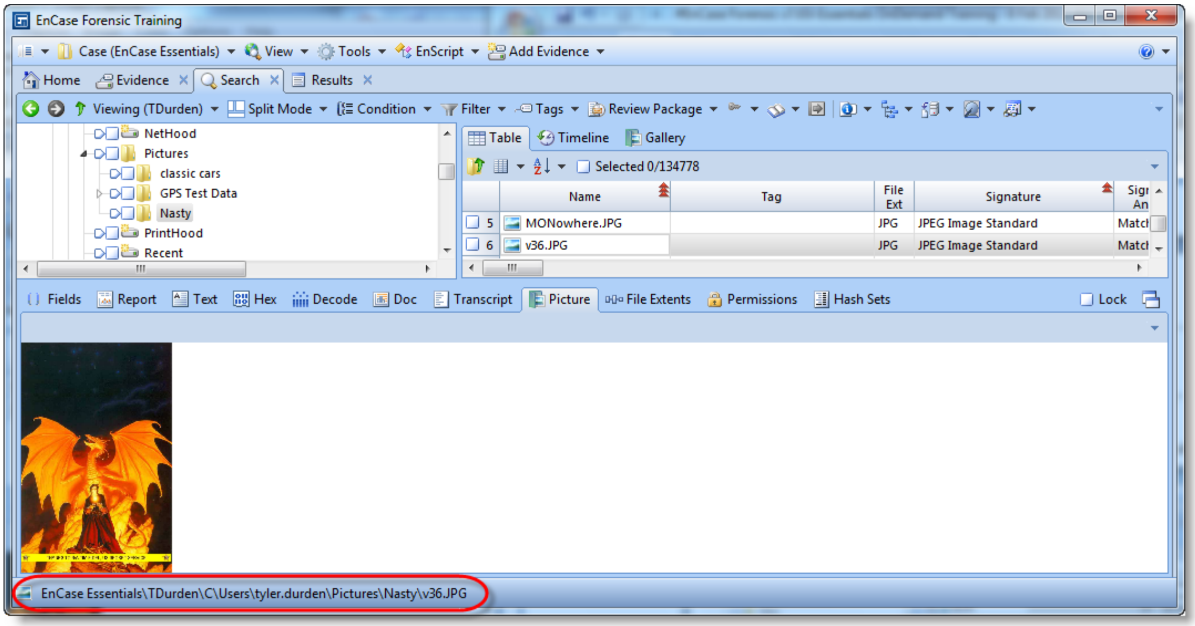
	Name	Tag	File Ext
34	Root Entry		
35	UsrClass.dat		dat
36	v36.JPG		JPG
37	v36.JPG		JPG
38	v8.jpg		jpg
39	v8.jpg		jpg

EnCase Essentials\TDurden\C\Users\tyler.durden\Pictures\Nasty\v36.JPG

Figure 6-19 Go to file

In this case, the file was located because it is in the folder called "Nasty." As you can see, the index allows searching on both file content and metadata.

If the file is a picture, you can use the Picture view in the View Pane to show the image.

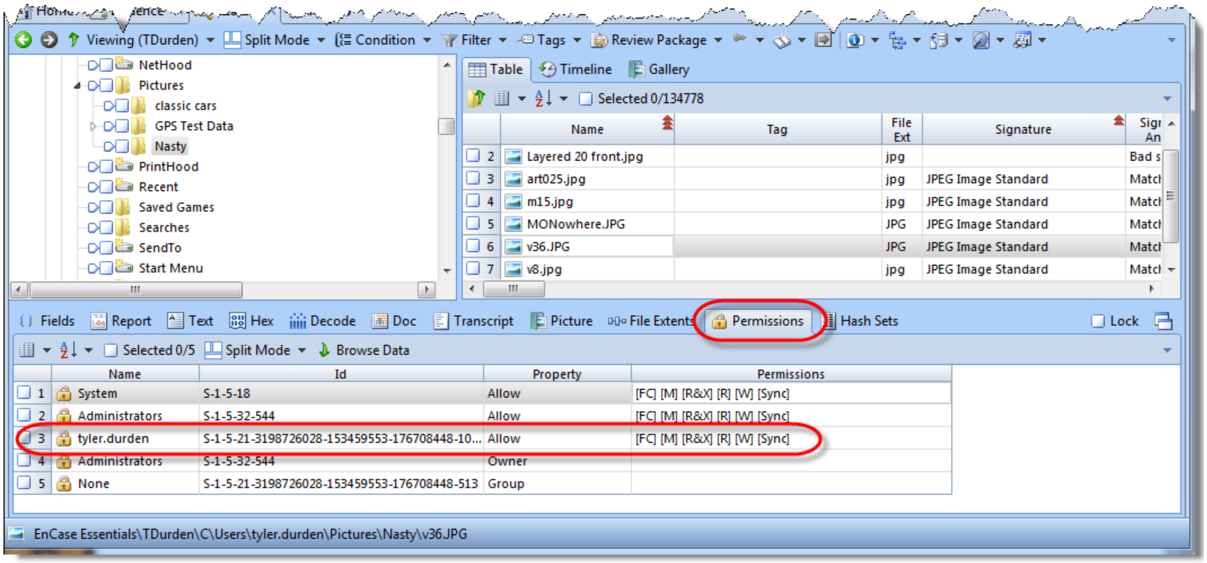


	Name	Tag	File Ext	Signature	Sig An
5	MONowhere.JPG		JPG	JPEG Image Standard	Match
6	v36.JPG		JPG	JPEG Image Standard	Match

EnCase Essentials\TDurden\C\Users\tyler.durden\Pictures\Nasty\v36.JPG

Figure 6-20 Gallery view

You can look at the **Permissions** tab to see that tyler.durden has access permission for the file.



	Name	Tag	File Ext	Signature	Sig An
2	Layered 20 front.jpg		jpg		Bad s
3	art025.jpg		jpg	JPEG Image Standard	Match
4	m15.jpg		jpg	JPEG Image Standard	Match
5	MONowhere.JPG		JPG	JPEG Image Standard	Match
6	v36.JPG		JPG	JPEG Image Standard	Match
7	v8.jpg		jpg	JPEG Image Standard	Match

	Name	Id	Property	Permissions
1	System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
2	Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
3	tyler.durden	S-1-5-21-3198726028-153459553-176708448-10...	Allow	[FC] [M] [R&X] [R] [W] [Sync]
4	Administrators	S-1-5-32-544	Owner	
5	None	S-1-5-21-3198726028-153459553-176708448-513	Group	

EnCase Essentials\TDurden\C\Users\tyler.durden\Pictures\Nasty\v36.JPG

Figure 6-21 File permissions

And then you may wish to add the evidence to your report template with a bookmark on all of the files.

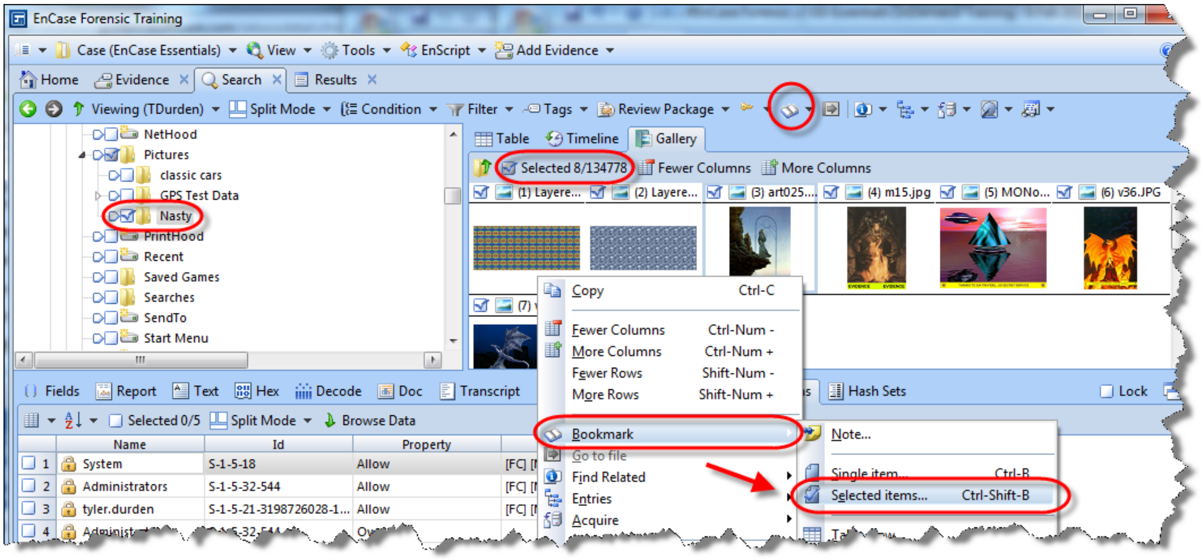


Figure 6-22 Bookmarking selected files

NOTE: If you bookmark several files, you are not able to add a Bookmark comment. If wish to add a comment, then bookmark a Single File.

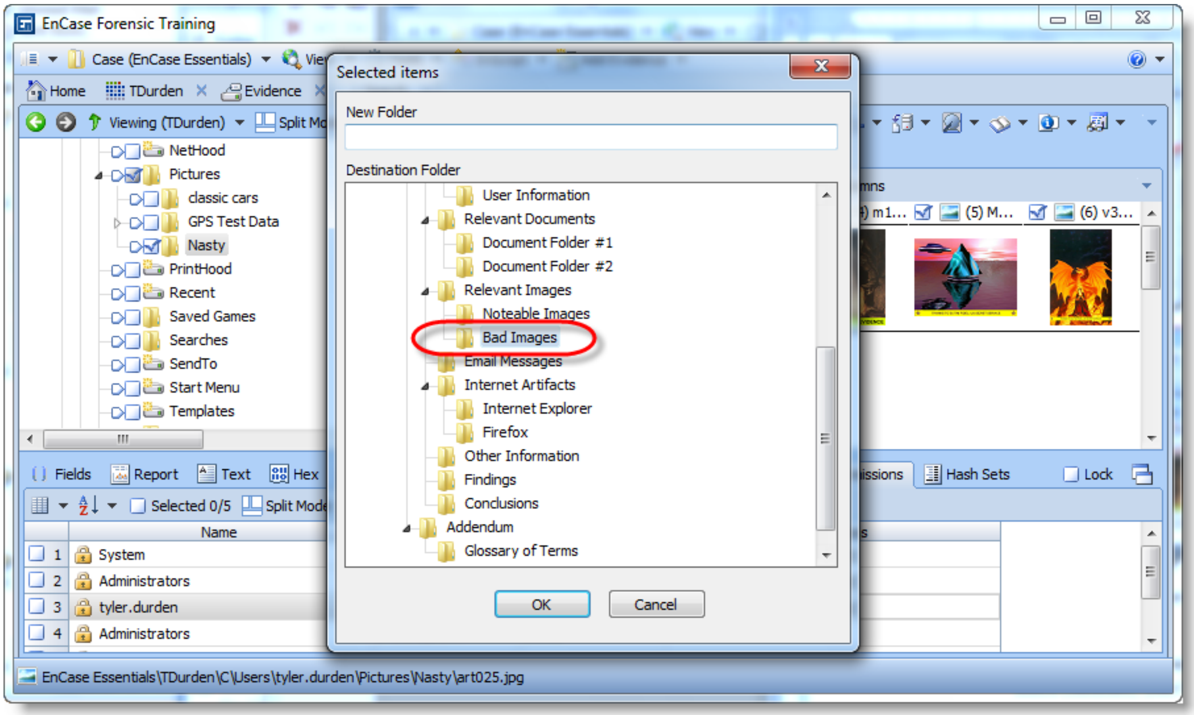


Figure 6-23 Bookmark Destination Folder

VIEWING KEYWORD SEARCH RESULTS

Once your case has been keyword searched for raw text, you can then search for desired information.

1. Click the **Search** button on the Home page

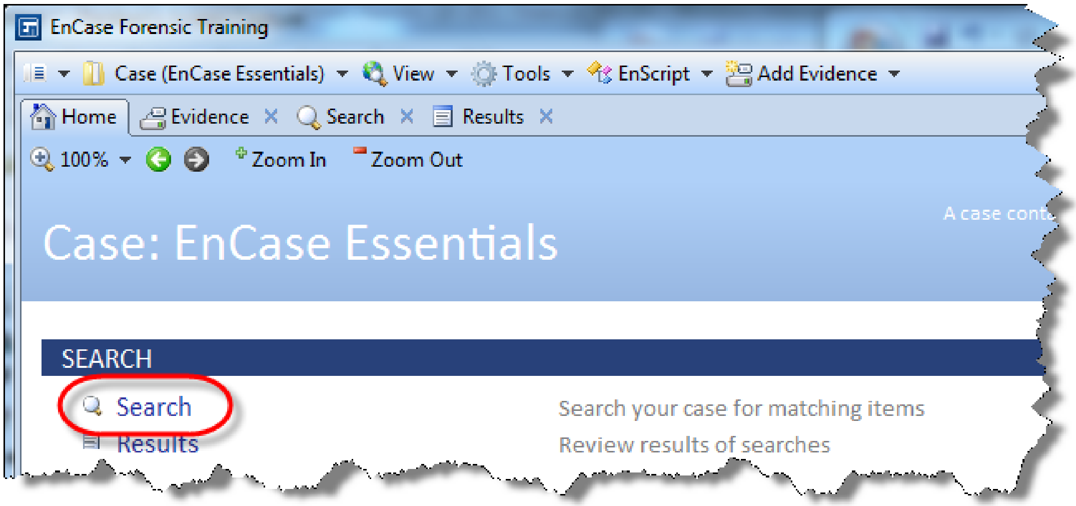


Figure 6-24 Search view

2. Click on the **Keywords** button to view the search results.

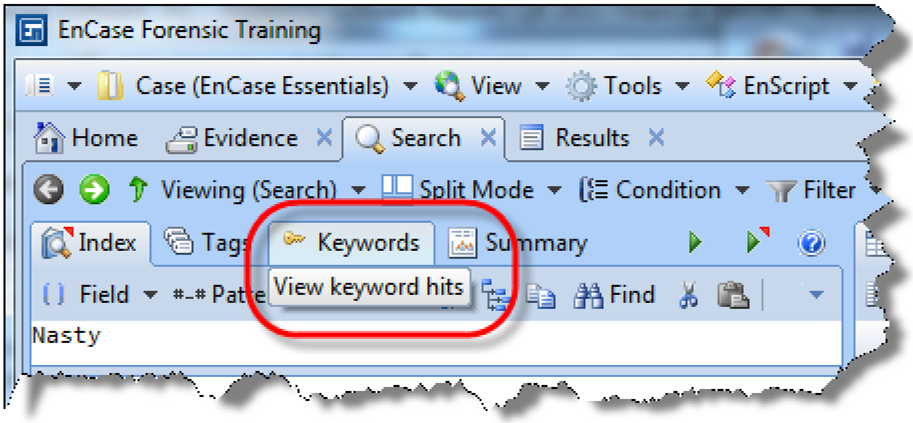
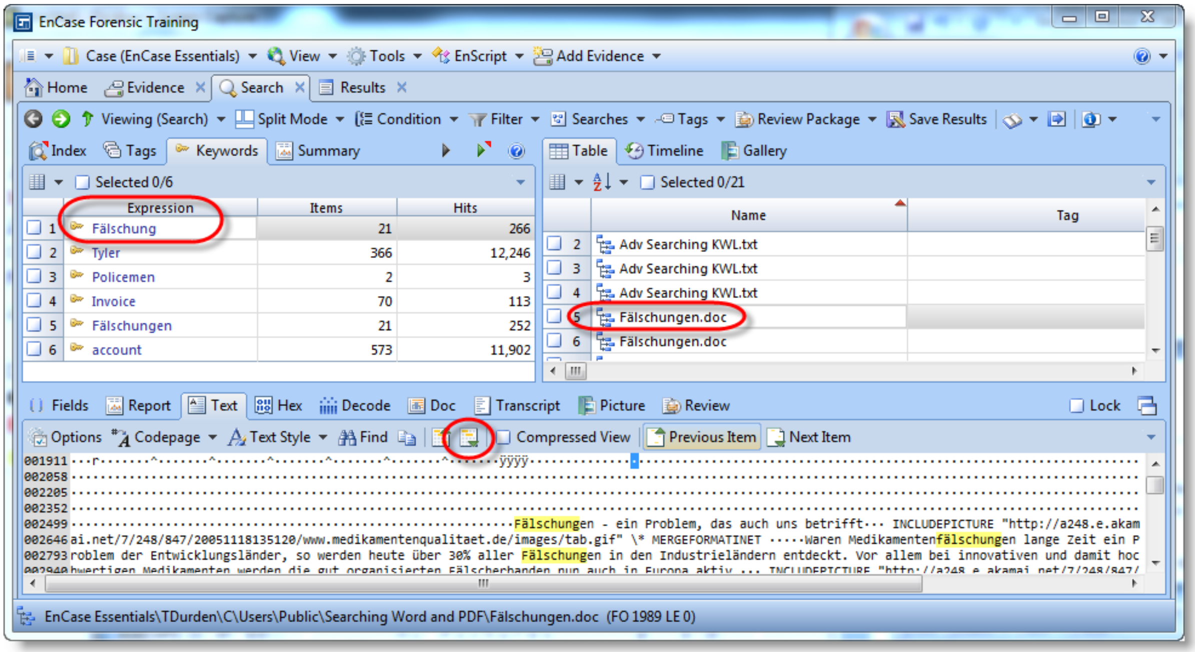


Figure 6-25 Keywords

3. Click on the hyperlink for the desired keyword to display the results in the Table Pane

You can review the file entries that contain the search term; for example, the document called “Fälschungen.doc” displays as is shown in the following screenshot. “Fälschungen” means “counterfeiting” in German.

Use the **Next Hit** button to view the search hit in a large file.


EnCase Forensic Training
Case (EnCase Essentials) View Tools EnScript Add Evidence
Home Evidence Search Results
Viewing (Search) Split Mode Condition Filter Searches Tags Review Package Save Results
Index Tags Keywords Summary
Table Timeline Gallery
Selected 0/6
Selected 0/21
Fields Report Text Hex Decode Doc Transcript Picture Review Lock
Options Codepage Text Style Find Compressed View Previous Item Next Item

	Expression	Items	Hits
1	Fälschung	21	266
2	Tyler	366	12,246
3	Policemen	2	3
4	Invoice	70	113
5	Fälschungen	21	252
6	account	573	11,902

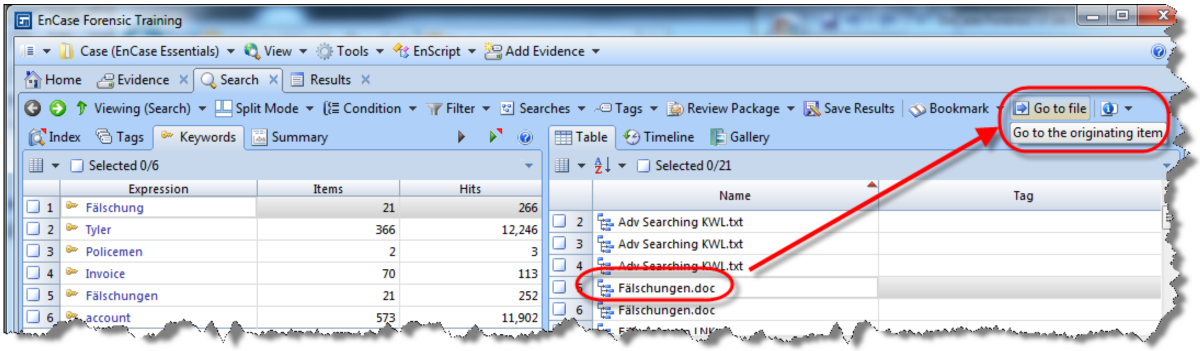
	Name	Tag
2	Adv Searching KWL.txt	
3	Adv Searching KWL.txt	
4	Adv Searching KWL.txt	
5	Fälschungen.doc	
6	Fälschungen.doc	

```
001911 ···r·······^·······^·······^·······^·······^·······^······ÿÿÿÿ··············································
002058 ·······················································································································
002205 ·······················································································································
002352 ·······················································································································
002499 ·······················································Fälschungen - ein Problem, das auch uns betrifft··· INCLUDEPICTURE "http://a248.e.akam
002646 ai.net/7/248/847/20051118135120/www.medikamentenqualitaet.de/images/tab.gif" \* MERGEFORMATINET ·····Waren Medikamentenfälschungen lange Zeit ein P
002793 roblem der Entwicklungsländer, so werden heute über 30% aller Fälschungen in den Industrieländern entdeckt. Vor allem bei innovativen und damit hoc
002940 hwertigen Medikamenten werden die gut organisierten Fälscherbanden nun auch in Europa aktiv ... INCLUDEPICTURE "http://a248.e.akamai.net/7/248/847/
```

EnCase Essentials\TDurden\C\Users\Public\Searching Word and PDF\Fälschungen.doc (FO 1989 LE 0)

Figure 6-26 Search result

To see the file in the context of the evidence, click on **Go to file**.

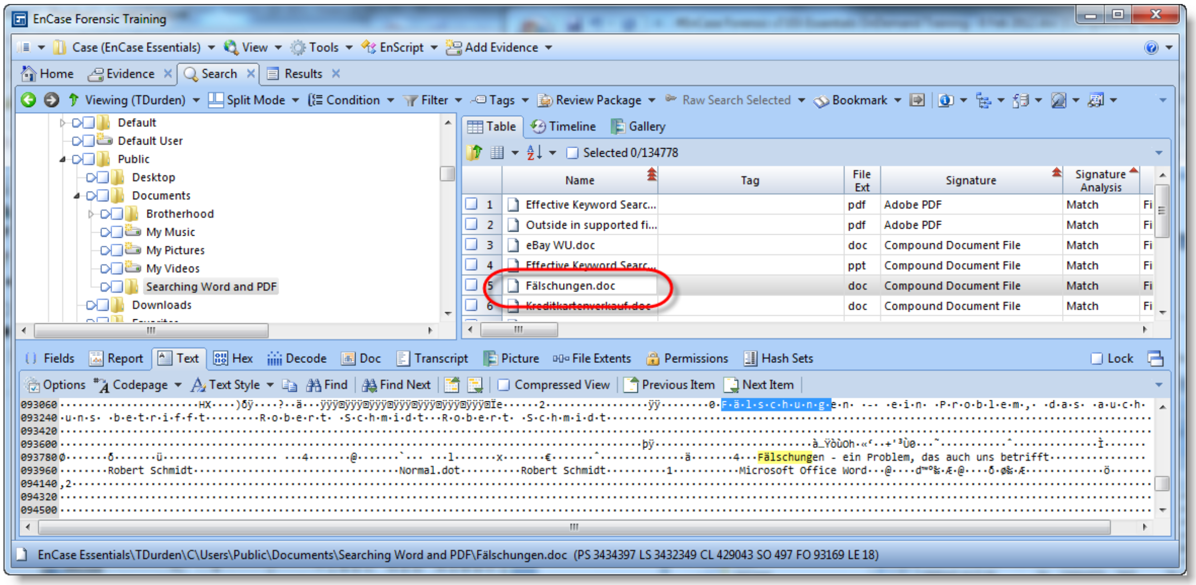

EnCase Forensic Training
Case (EnCase Essentials) View Tools EnScript Add Evidence
Home Evidence Search Results
Viewing (Search) Split Mode Condition Filter Searches Tags Review Package Save Results Bookmark Go to file
Go to the originating item
Index Tags Keywords Summary
Table Timeline Gallery
Selected 0/6
Selected 0/21

	Expression	Items	Hits
1	Fälschung	21	266
2	Tyler	366	12,246
3	Policemen	2	3
4	Invoice	70	113
5	Fälschungen	21	252
6	account	573	11,902

	Name	Tag
2	Adv Searching KWL.txt	
3	Adv Searching KWL.txt	
4	Adv Searching KWL.txt	
5	Fälschungen.doc	
6	Fälschungen.doc	

Figure 6-27 Go to file

You will be taken to the Entries view of the Search tab to analyze the evidence in context.



		Name	Tag	File Ext	Signature	Signature Analysis	
□	1	Effective Keyword Searc...		pdf	Adobe PDF	Match	Fi
□	2	Outside in supported fi...		pdf	Adobe PDF	Match	Fi
□	3	eBay WU.doc		doc	Compound Document File	Match	Fi
□	4	Effective Keyword Searc...		ppt	Compound Document File	Match	Fi
□	5	Fälschungen.doc		doc	Compound Document File	Match	Fi
□	6	Kreditkartenverkauf.doc		doc	Compound Document File	Match	Fi

```
093060 ·····················HX····)õÿ····?··ä···ÿÿÿ¤ÿÿÿ¤ÿÿÿ¤ÿÿÿ¤ÿÿÿ¤ÿÿÿ¤ÿÿÿ¤Ïe······2················ÿÿ········0·F·ä·l·s·c·h·u·n·g·e·n· ·-· ·e·i·n· ·P·r·o·b·l·e·m·,· ·d·a·s· ·a·u·c·h·
093240 ·u·n·s· ·b·e·t·r·i·f·f·t········R·o·b·e·r·t· ·S·c·h·m·i·d·t···R·o·b·e·r·t· ·S·c·h·m·i·d·t·······································
093420 ································································································································
093600 ·······························································þÿ·····················à_ŸòùOh·«ʻ··+'³Ù0···˜···········ˆ·········Ì·······
093780 Ø······ð······ü················ ···4······@······`··· ···l······x······€······ˆ·············ä······4···Fälschungen - ein Problem, das auch uns betrifft···········
093960 ·······Robert Schmidt······························Normal.dot·········Robert Schmidt·········1·········Microsoft Office Word···@····d™º%·Æ·@····ð·ø%·Æ··············ö·······
094140 ,2······························································································································
094320 ································································································································
094500 ································································································································
```

EnCase Essentials\TDurden\C\Users\Public\Documents\Searching Word and PDF\Fälschungen.doc (PS 3434397 LS 3432349 CL 429043 SO 497 FO 93169 LE 18)

Figure 6-28 File in context of entries

Use the **Back** button to return to the Search view.

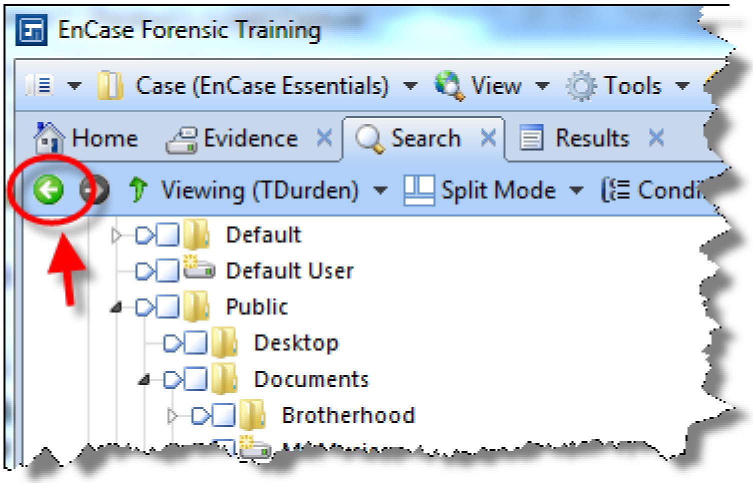


Figure 6-29 Back to Search query

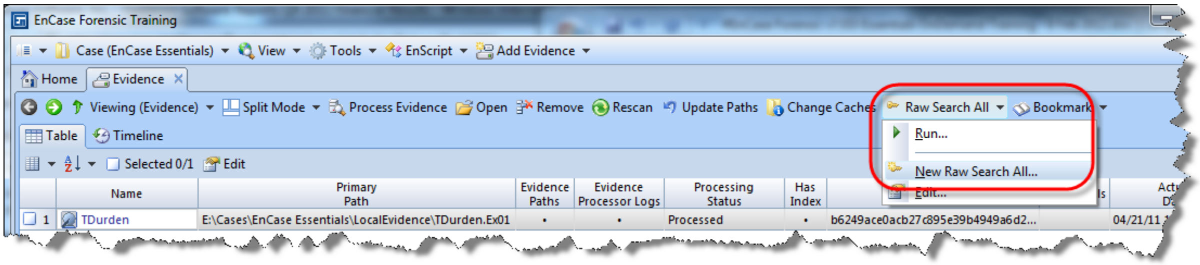
Raw Searches

Although index searching is the recommended type of search, there may be times when you want to perform a search across the raw contents of a device. In those cases, you can perform a keyword or non-indexed search on your case data. Because keyword searching only searches the raw binary form of a file, some content may not be discovered if it is compressed or obfuscated.

To perform a raw keyword search on your data, make sure that your case contains the device that you want to search.

For information, see the **Search for Keywords** option of the Evidence Processor. In addition to keyword searching using the Evidence Processor, you can also initiate a raw keyword search of one or more devices from the **Evidence** tab. To initiate a search in this manner, follow these steps:

1. Navigate to the **Evidence** tab and then to the top level of the tab (using the **View** drop-down menu on the tab toolbar)
2. Select the device or devices that you wish to search using the checkboxes on the left side of the table
3. Select **Raw Search All** from the tab toolbar

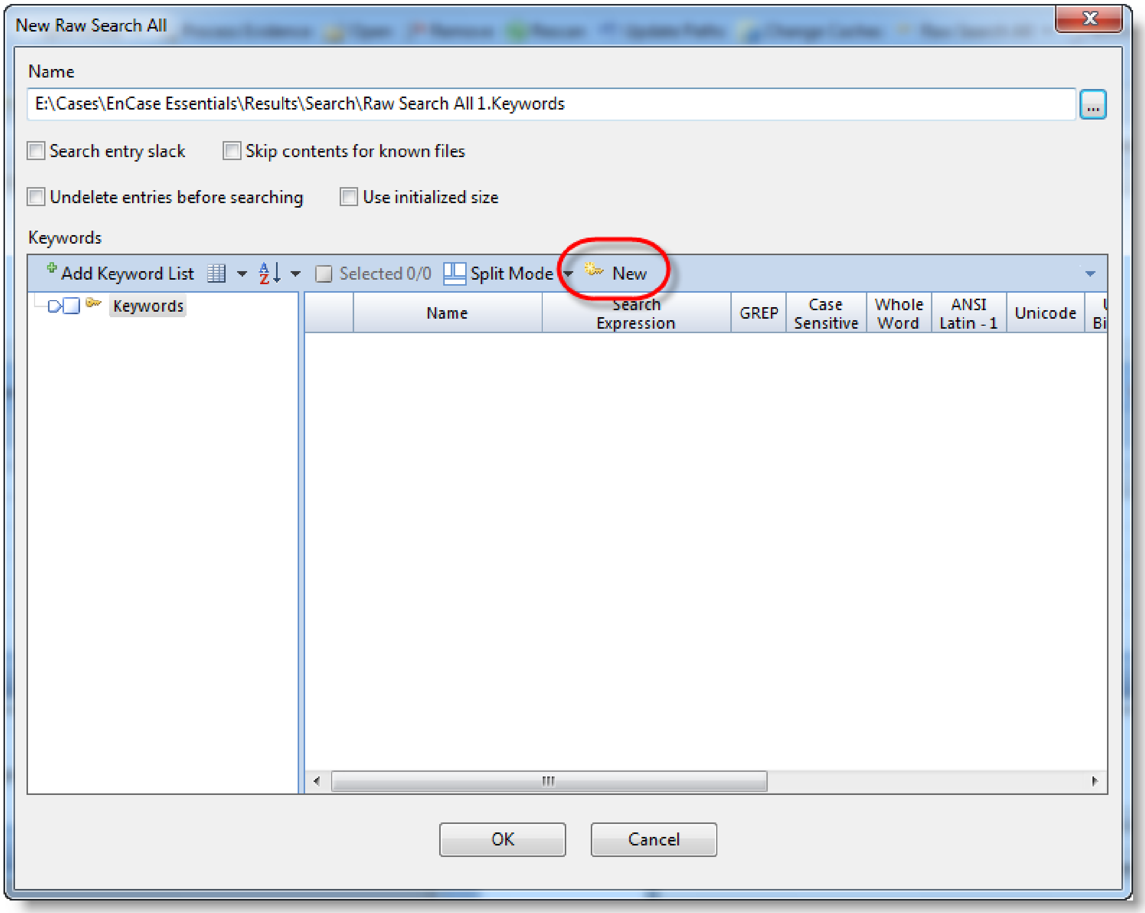


	Name	Primary Path	Evidence Paths	Evidence Processor Logs	Processing Status	Has Index		Act D
□ 1	TDurden	E:\Cases\EnCase Essentials\LocalEvidence\TDurden.Ex01	•	•	Processed	•	b6249ace0acb27c895e39b4949a6d2...	04/21/11

Figure 6-30 New Keyword Search All Entries...

4. Select a previously run search or create a new search

5. Add the keywords and options that you wish to use just like in the Evidence Processor and select **OK**



New Raw Search All

Name

E:\Cases\EnCase Essentials\Results\Search\Raw Search All 1.Keywords

□ Search entry slack □ Skip contents for known files

□ Undelete entries before searching □ Use initialized size

Keywords

Figure 6-31 Edit Keywords dialog

Case and Evidence Keywords

Keyword searches that are ***not*** initiated from the Evidence Processor are stored with the case and are case specific.

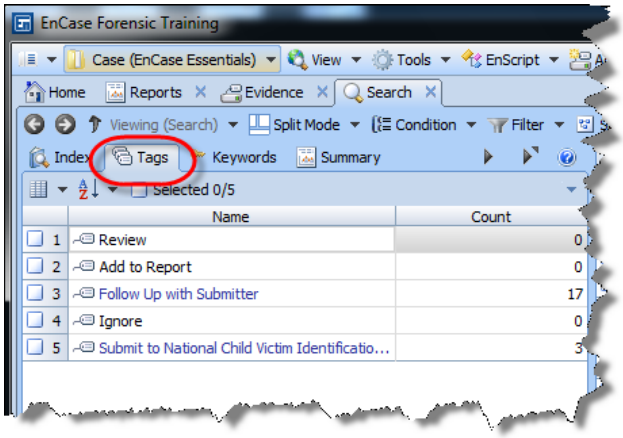
Keyword searches that are conducted with the Evidence Processor are stored with the device's cache files and can be used with any number of cases.

Tag Searches

EnCase v7 also provides the capability to search for instances of a particular tag that you have created. Suppose you create a collection of three tags associated with pieces of evidence, one of which is named “Submit to National Child Victim Identification Program.”

You can search through your evidence for all instances of that tag and the result set that displays will consist only of evidence with that tag.

You can also tag files in this view. For more information, see Lesson 9, *Bookmarking and Tagging Your Findings*.

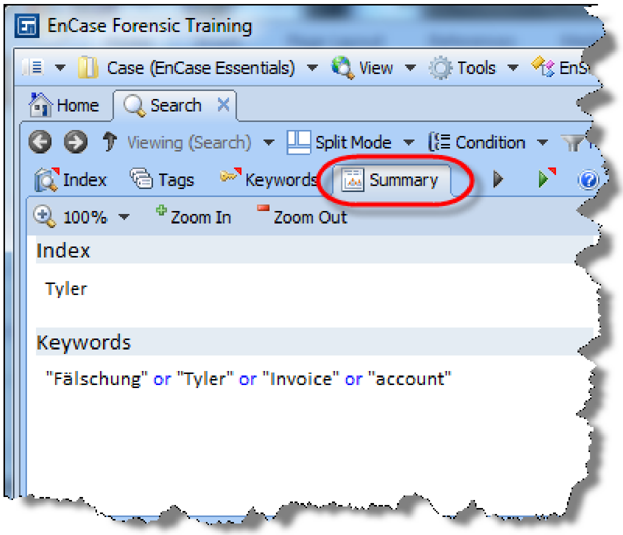


	Name	Count
1	Review	0
2	Add to Report	0
3	Follow Up with Submitter	17
4	Ignore	0
5	Submit to National Child Victim Identificatio…	3

Figure 6-32 Tag Searches

Search Summary

To see a description of all active search criteria click the **Summary** tab.



Index

Tyler

Keywords

"Fälschung" or "Tyler" or "Invoice" or "account"

Figure 6-33 Search Summary

Notes

Notes

Processed Evidence Results

File Types

When an evidence file is opened in EnCase® v7, the file system contained on the device is parsed and displayed for browsing in the Evidence→Viewing (Entry) tab. Files may be navigated and viewed in the table area of the **Table Pane**. EnCase v7 displays files, folders, and other objects on the media, including those that are deleted or overwritten, by maintaining invalid starting cluster addresses as well as other attributes or characteristics.

The **Description** column provides information regarding the object's attributes, status (allocated or deleted), and other details dependent upon what the entry represents.

To remove unnecessary complexity in EnCase v7, the **File Types**, **File Viewers**, and **File Signatures** tables in previous versions of EnCase® software are now contained in one location, the **File Types** view.

Click on the **View** menu and select **File Types**.

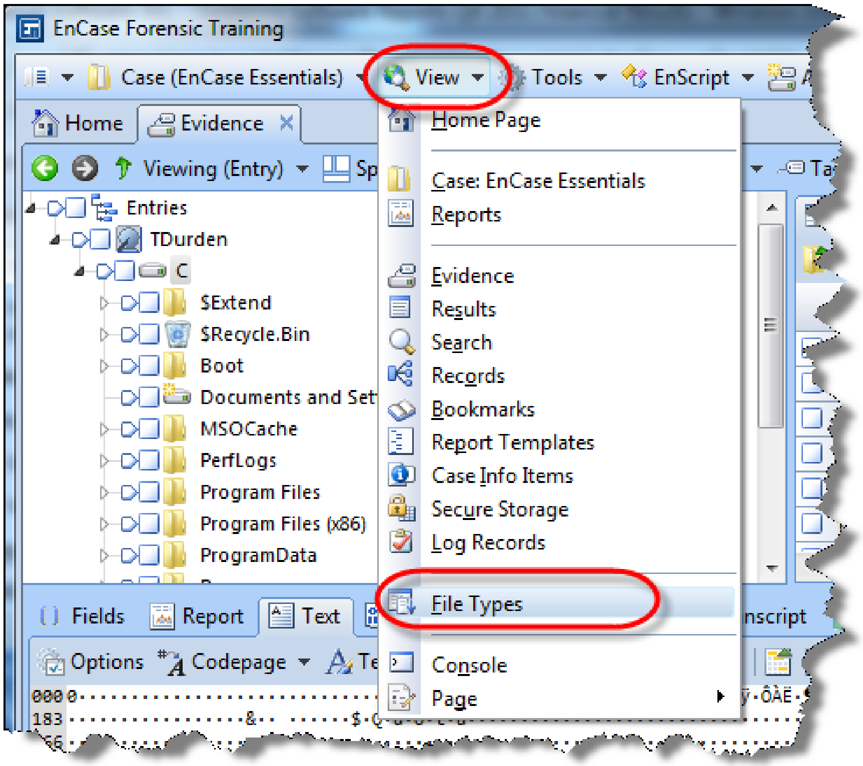


Figure 7-1 File Types and Entry Description column

File Signatures

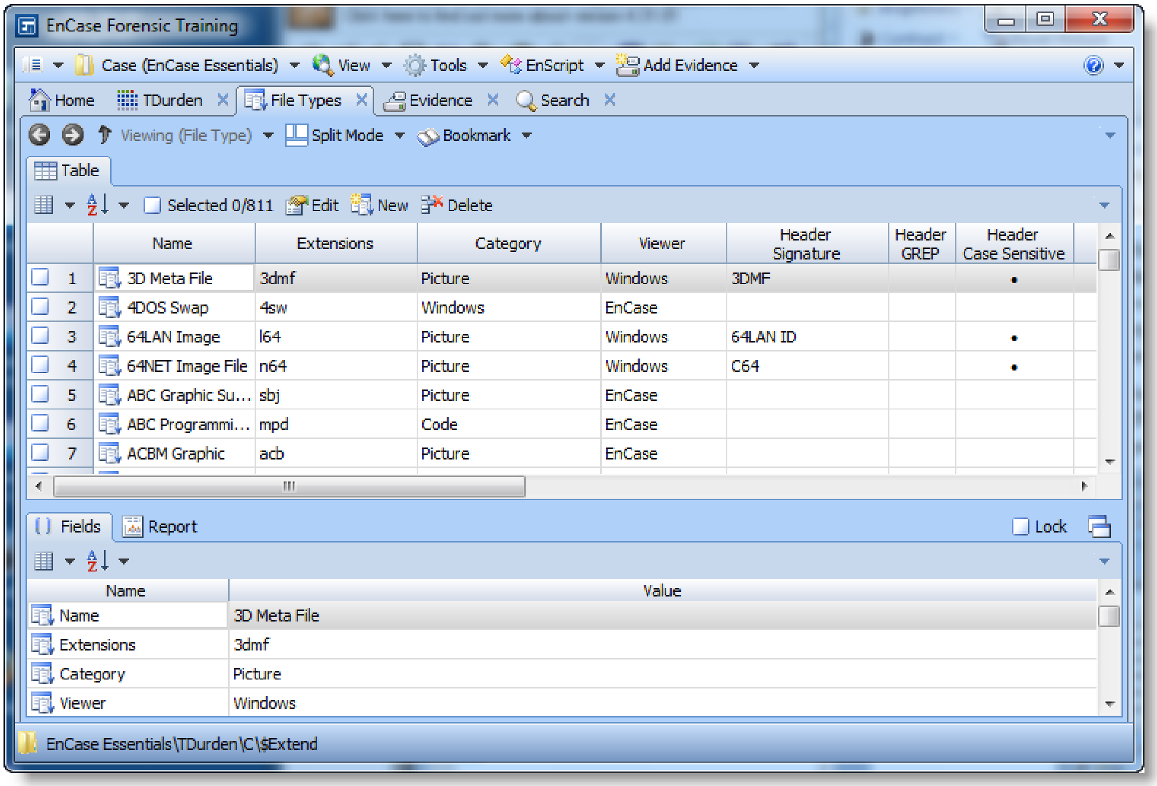
As stated previously, the File Signatures table has been incorporated into **File Types** in EnCase v7.

There are thousands of file types. Some file types have been standardized. The International Standards Organization (ISO) and the International Telecommunications Union, Telecommunication Standardization Sector (ITU-T) are working to standardize different types of electronic data. Typical graphical images, such as the JPEG (Joint Photographic Experts Group), have been standardized by both of these organizations. When file types become standardized, a signature or header that programs can recognize usually precedes the data.

File headers are the first few bytes of a file and are associated with specific file extensions.

File extensions are the three or four characters that follow the last dot in a filename. They reveal the type of data that the file represents. If one were to see a .TXT extension, a data type of text would be expected. Many programs rely specifically on the extension to reflect the proper data type. Windows, for example, associates file types with applications programs by use of file extensions.

Some users have been known to change file extensions to hide the true nature of the files. A JPEG (image file) that has an incorrect extension, such as .DLL, will not be recognized by most programs as a picture.



		Name	Extensions	Category	Viewer	Header Signature	Header GREP	Header Case Sensitive
□	1	3D Meta File	3dmf	Picture	Windows	3DMF		•
□	2	4DOS Swap	4sw	Windows	EnCase			
□	3	64LAN Image	l64	Picture	Windows	64LAN ID		•
□	4	64NET Image File	n64	Picture	Windows	C64		•
□	5	ABC Graphic Su…	sbj	Picture	EnCase			
□	6	ABC Programmi…	mpd	Code	EnCase			
□	7	ACBM Graphic	acb	Picture	EnCase			

Name	Value
Name	3D Meta File
Extensions	3dmf
Category	Picture
Viewer	Windows

Figure 7-2 File Types

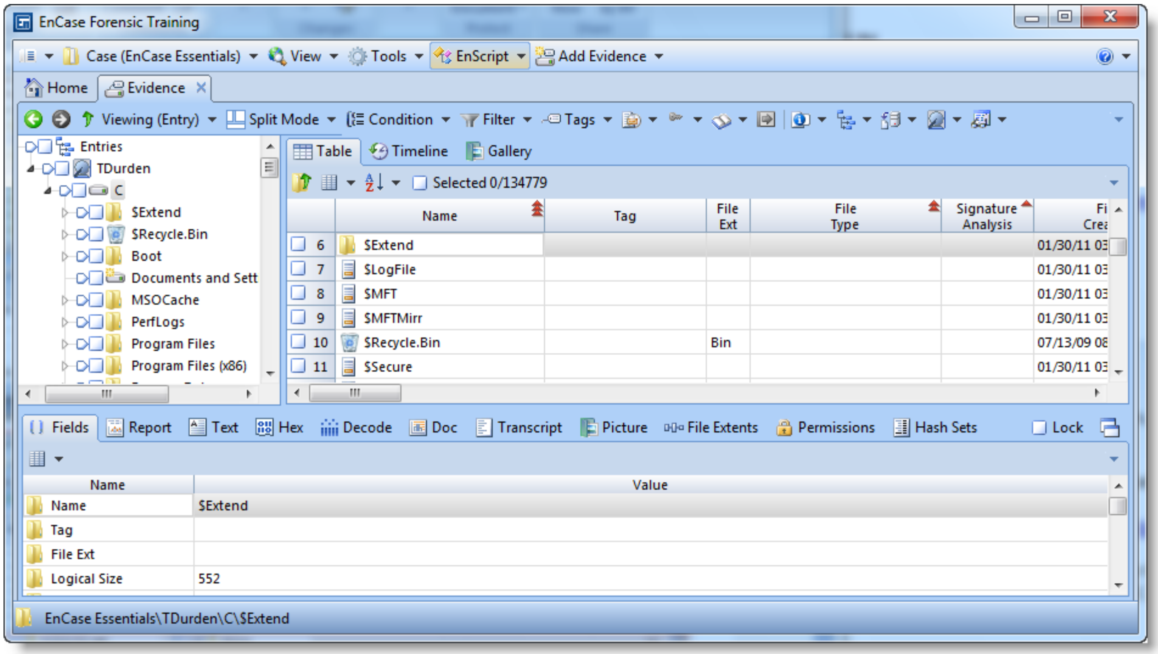
By default EnCase v7 displays graphic files, such as that mentioned in the previous example, in the Gallery view based on their extensions. By running the file signature analysis process, EnCase v7 compares the file's signature with the extension of the file, and then compares both with the File Types table to determine if the file extension has been changed. This process is essential to properly identify and classify files on a subject's hard drive.

File Types table contains the following information about each type of file:

- **Name (required)** – Name of the file type
- **Extensions (Extensions or Header required)** – Extension(s) of the file type
- **Category (required)** – The category of the file (used for the Entry Description)
- **Viewer (required)** – The default viewer if the file is opened from EnCase v7
- **Header Signature (Extensions or Header required)** – Header associated with the file type; may be a keyword string or GREP expression
- **Header GREP** – True or false for correct searching/analysis
- **Header Case Sensitive** – True or false for correct searching/analysis
- **Footer Signature** – If available; used for file carving
- **Footer GREP** – True or false for correct searching/analysis
- **Footer Case Sensitive** – True or false for correct searching/analysis
- **Unique Tag** – Allows filtering for the file type tag (signature) with a unique tag name for the file type
- **Default Length** – 0 unless changed by user
- **User Defined** – If you edit or create a new a file type, it will be marked *True* as user defined (this will prevent it from being overwritten when an update is released by Guidance Software)
- **Disabled** – Check the box to disable the File Type for file signature analysis

Before a File Signature Analysis is run with the Evidence Processor, the Evidence tab Entry columns will display the following:

- **Signature Analysis**
  - Blank
- **File Type**
  - Blank



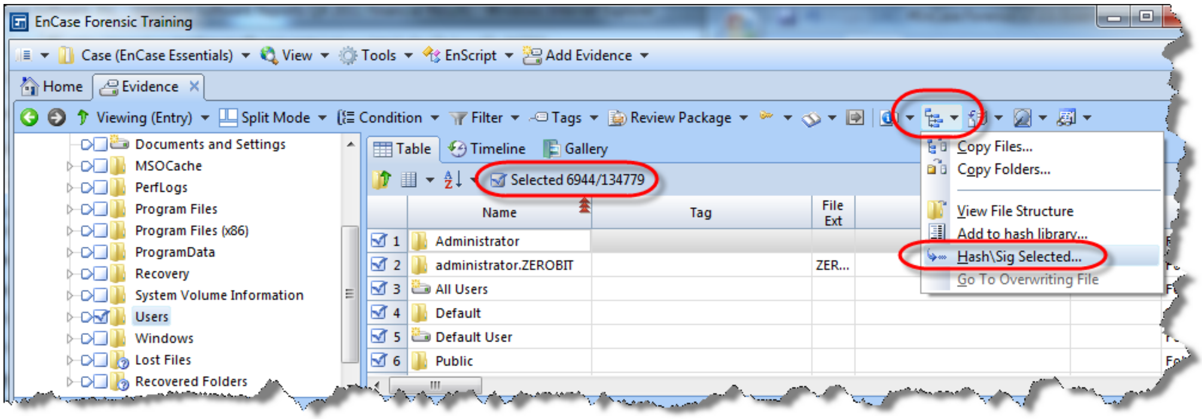
	Name	Tag	File Ext	File Type	Signature Analysis	Fi Crea
6	$Extend					01/30/11 03
7	$LogFile					01/30/11 03
8	$MFT					01/30/11 03
9	$MFTMirr					01/30/11 03
10	$Recycle.Bin		Bin			07/13/09 08
11	$Secure					01/30/11 03

Name	Value
Name	$Extend
Tag	
File Ext	
Logical Size	552

EnCase Essentials\TDurden\C\$Extend

Figure 7-3 Before file Signature Analysis

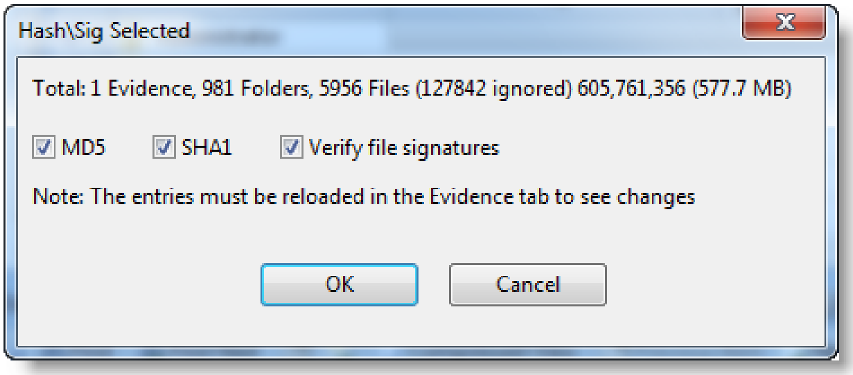
You can also run the File Signature and Hash Analysis independent of the Evidence Processor. Select the desired files and choose the **Entries** drop-down menu. Select **Hash\Sig Selected…**



	Name	Tag	File Ext
☑ 1	Administrator		
☑ 2	administrator.ZEROBIT		ZER...
☑ 3	All Users		
☑ 4	Default		
☑ 5	Default User		
☑ 6	Public		

Figure 7-4 Hash\Sig Selected Files

Select the options for hashing and file signatures and click **OK**.



Total: 1 Evidence, 981 Folders, 5956 Files (127842 ignored) 605,761,356 (577.7 MB)

☑ MD5 ☑ SHA1 ☑ Verify file signatures

Note: The entries must be reloaded in the Evidence tab to see changes

Figure 7-5 Hash\Sig Selected Options

After Signature Analysis, the columns will display the results of the analysis:

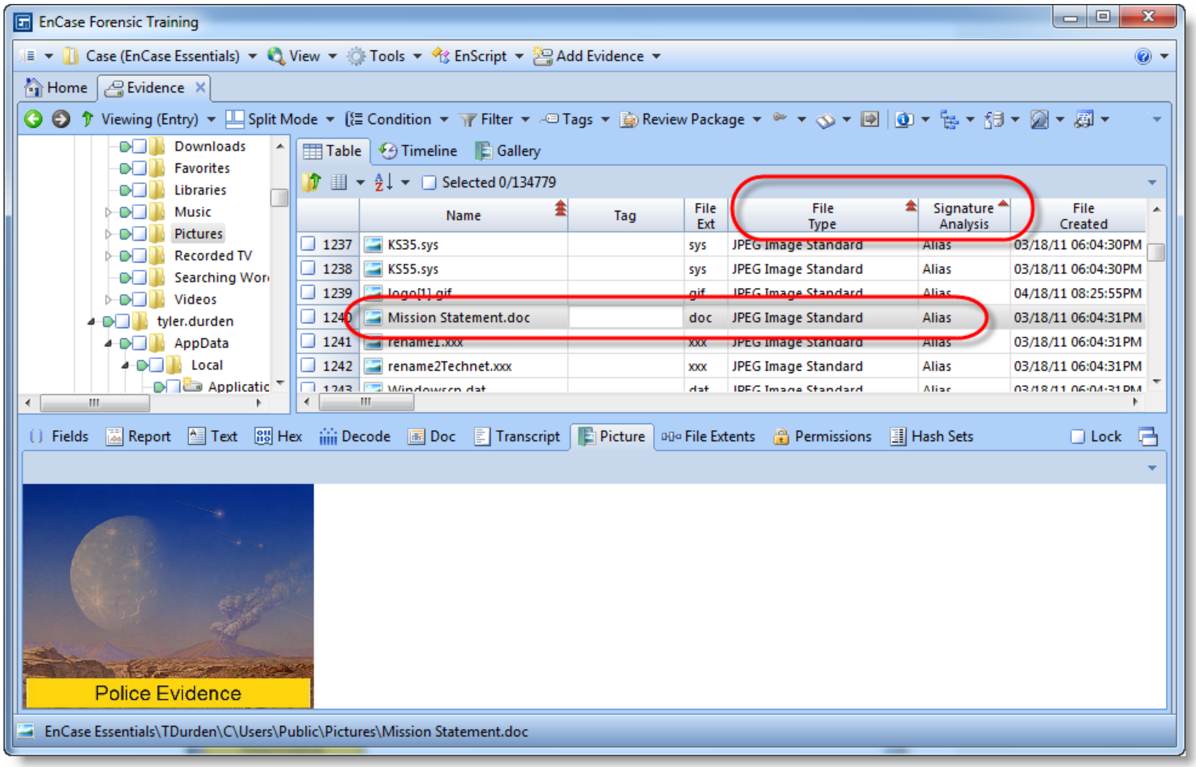
- **Signature Analysis**
    - Displays the results of a Signature Analysis
        - **Match**
            - Signature matches a File Type Header and the Extension is included in the extensions for that File Type
            - Signature does not match any File Type Header, but there is a File Type that matches the extension
            - A .txt file with data at the beginning of the file not defined as a header within the File Signatures table is identified as a Match
        - **Alias**
            - Signature matches a File Type Search Expression Header, but the extension is not included in the extensions for that File Type
        - **Bad Signature**
            - Signature does not match any File Type Header, but there is a matching File Type Extension
        - **Unknown**
            - Signature does not match any File Type Header and there is no matching File Type Extension
- **File Type** (formerly Signature)
    - If Signature Analysis records a Match or Alias, EnCase v7 will display the File Type property of the File Type associated with the Signature Analysis

Now that the columns are aligned, start examining the file signatures. Use the **Set Included Folders** option to display all entries in the Table view. Sort the columns in the following order:

- First level – Signature Analysis
- Second level – File Type
- Third level – Name

The arrows on each column heading should appear as they are displayed in the following screenshot.

NOTE: Shift-double-click to enable secondary sorts.



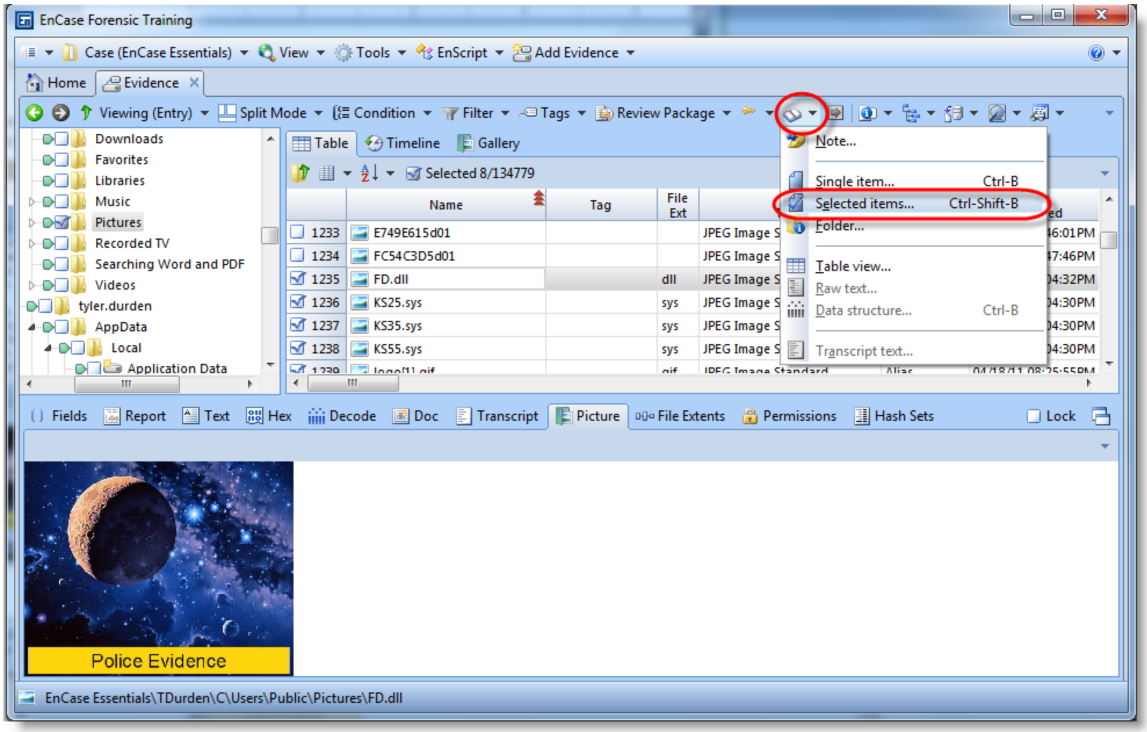
	Name	Tag	File Ext	File Type	Signature Analysis	File Created
1237	KS35.sys		sys	JPEG Image Standard	Alias	03/18/11 06:04:30PM
1238	KS55.sys		sys	JPEG Image Standard	Alias	03/18/11 06:04:30PM
1239	logo[1].gif		gif	JPEG Image Standard	Alias	04/18/11 08:25:55PM
1240	Mission Statement.doc		doc	JPEG Image Standard	Alias	03/18/11 06:04:31PM
1241	rename1.xxx		xxx	JPEG Image Standard	Alias	03/18/11 06:04:31PM
1242	rename2Technet.xxx		xxx	JPEG Image Standard	Alias	03/18/11 06:04:31PM
1243	Windowscp.dat		dat	JPEG Image Standard	Alias	03/18/11 06:04:31PM

EnCase Essentials\TDurden\C\Users\Public\Pictures\Mission Statement.doc

Figure 7-6 After File Signature Analysis

To examine the signatures, scroll up or down while viewing the Signature column.

You can bookmark discovered evidence items. Blue-check the entries, right-click, and choose **Bookmark→Selected Items…** You can also use the **Bookmark** drop-down on the menu bar.



	Name	Tag	File Ext		
☐ 1233	E749E615d01			JPEG Image S	46:01PM
☐ 1234	FC54C3D5d01			JPEG Image S	47:46PM
☑ 1235	FD.dll		dll	JPEG Image S	04:32PM
☑ 1236	KS25.sys		sys	JPEG Image S	04:30PM
☑ 1237	KS35.sys		sys	JPEG Image S	04:30PM
☑ 1238	KS55.sys		sys	JPEG Image S	04:30PM

EnCase Essentials\TDurden\C\Users\Public\Pictures\FD.dll

Figure 7-7 Bookmark→Selected Items…

Choose the appropriate Destination Folder in the Report template.

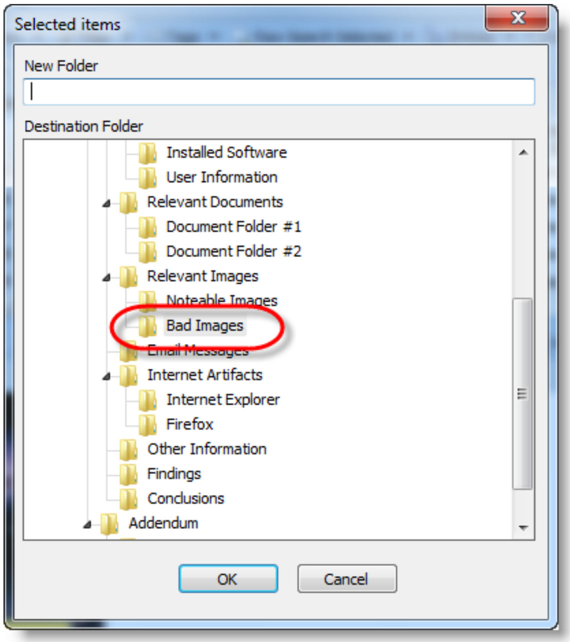
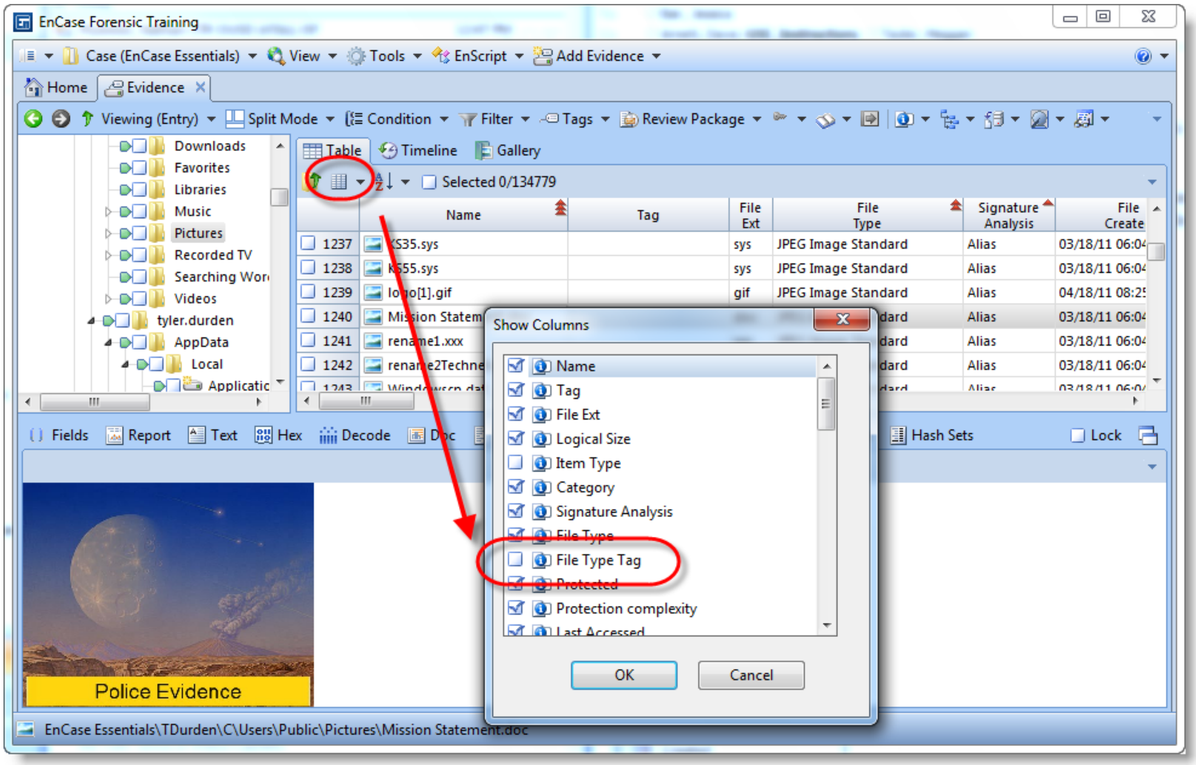


Figure 7-8 Destination Folder

You can also activate the File Type Tag column to aid in your investigation. This will show you the Unique Tag for the File Type validated in the File Signature Analysis.



□ Selected 0/134779

	Name	Tag	File Ext	File Type	Signature Analysis	File Create
1237	KS35.sys		sys	JPEG Image Standard	Alias	03/18/11 06:04
1238	KS55.sys		sys	JPEG Image Standard	Alias	03/18/11 06:04
1239	logo[1].gif		gif	JPEG Image Standard	Alias	04/18/11 08:25
1240	Mission Statem			dard	Alias	03/18/11 06:04
1241	rename1.xxx			dard	Alias	03/18/11 06:04
1242	rename2Techne			dard	Alias	03/18/11 06:04
1243	Windowscn.dat			dard	Alias	03/18/11 06:04

Show Columns

☑ Name
☑ Tag
☑ File Ext
☑ Logical Size
□ Item Type
☑ Category
☑ Signature Analysis
☑ File Type
□ File Type Tag
☑ Protected
☑ Protection complexity
☑ Last Accessed

OK Cancel

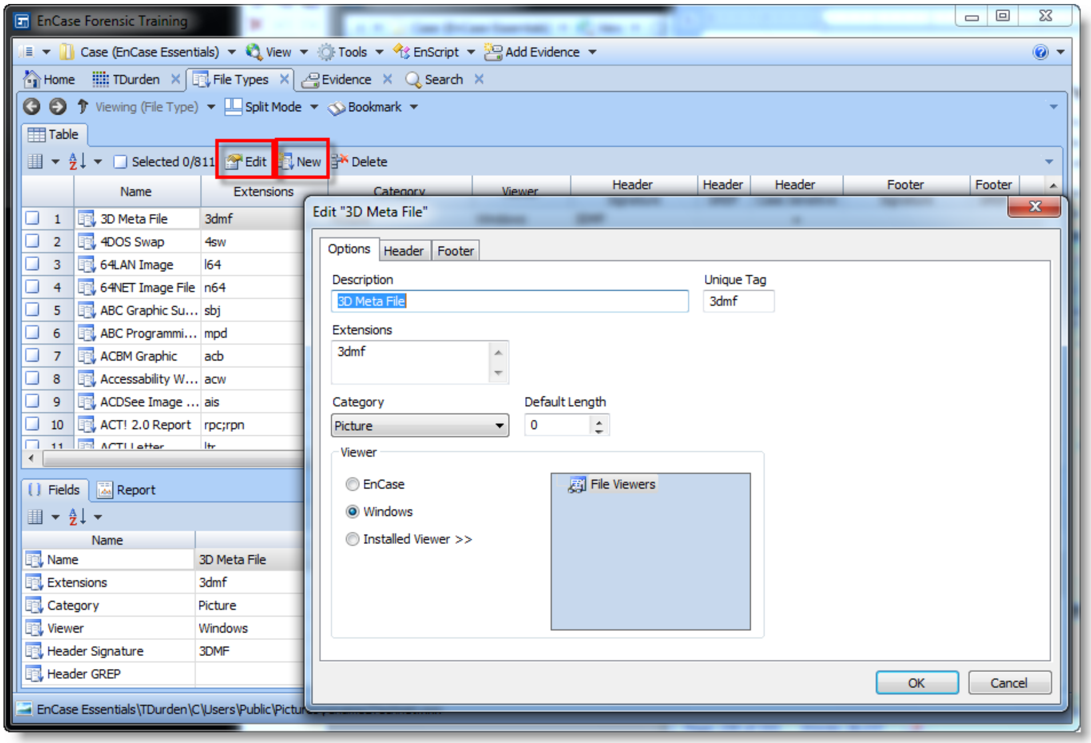
EnCase Essentials\TDurden\C\Users\Public\Pictures\Mission Statement.doc

Figure 7-9 File Type Tag

Adding / Editing a File Type

It is likely you will need to edit something within the File Types table or you may need to create a new entry within the table. The following example shows you how to edit an entry in the table. You would use the same steps in adding a new entry.

Edit a signature by selecting directly within the appropriate row and clicking **Edit**. Click on the **New** button above the File Types table to add a new entry.



	Name	Extensions
1	3D Meta File	3dmf
2	4DOS Swap	4sw
3	64LAN Image	l64
4	64NET Image File	n64
5	ABC Graphic Su…	sbj
6	ABC Programmi…	mpd
7	ACBM Graphic	acb
8	Accessability W…	acw
9	ACDSee Image …	ais
10	ACT! 2.0 Report	rpc;rpn
11	ACT! Letter	ltr

Edit "3D Meta File"

Options | Header | Footer

Description: 3D Meta File

Unique Tag: 3dmf

Extensions: 3dmf

Category: Picture

Default Length: 0

Viewer

○ EnCase
● Windows
○ Installed Viewer >>

File Viewers

Name	
Name	3D Meta File
Extensions	3dmf
Category	Picture
Viewer	Windows
Header Signature	3DMF
Header GREP	

Figure 7-10 Editing a File Type

Processed Evidence

The processed evidence will be found under the **Records** view.

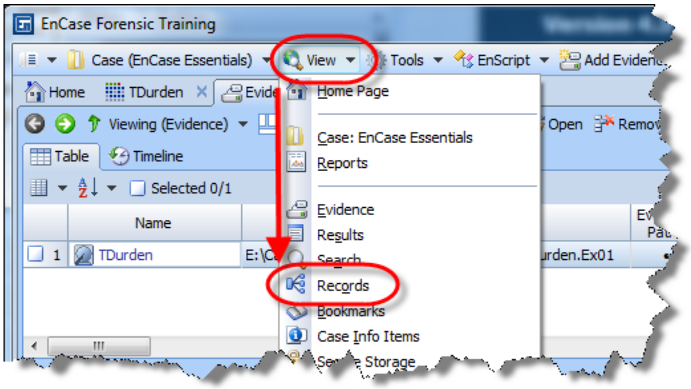
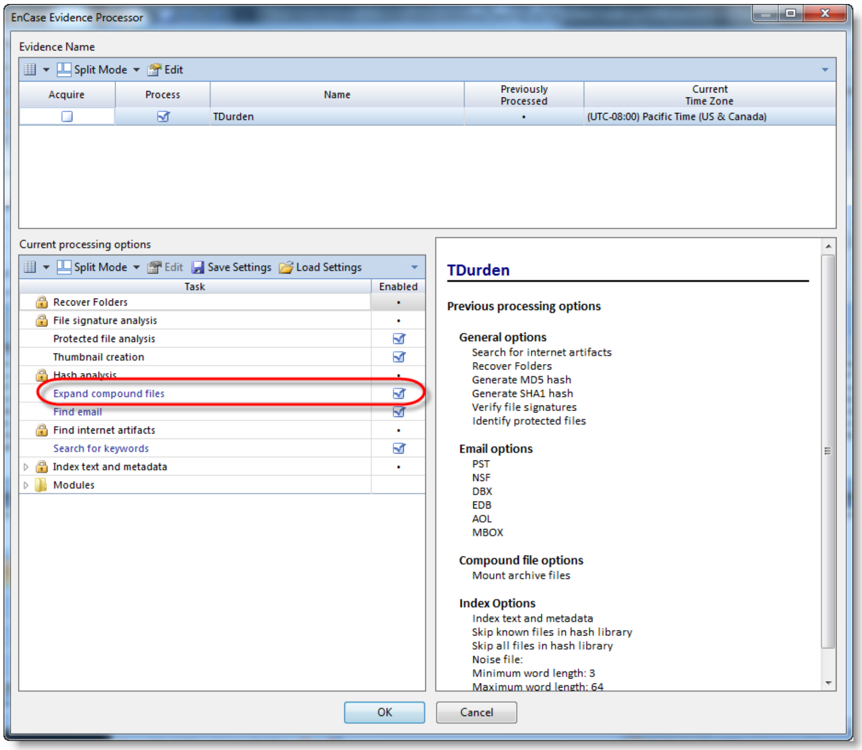


Figure 7-11 Records view

COMPOUND (COMPRESSED ARCHIVE) FILES

In EnCase® v6, mounted compound (compressed archive) files were held in memory, so you could have access to all the data in the case at once. However when you tried to mount numerous large archive files, you would run into system limitations. This would also cause the case file to open very slowly as the archive files were mounted into RAM.

In EnCase v7 you are able to view all available archives found and processed in the EnCase® Evidence Processor. As a reminder, we selected the **Expand compound files** task with the **Archives** as a file type.



Evidence Name

Acquire	Process	Name	Previously Processed	Current Time Zone
□	☑	TDurden	•	(UTC-08:00) Pacific Time (US & Canada)

Current processing options

Task	Enabled
Recover Folders	•
File signature analysis	•
Protected file analysis	☑
Thumbnail creation	☑
Hash analysis	•
Expand compound files	☑
Find email	☑
Find internet artifacts	•
Search for keywords	☑
Index text and metadata	•
Modules	

TDurden

Previous processing options

General options
Search for internet artifacts
Recover Folders
Generate MD5 hash
Generate SHA1 hash
Verify file signatures
Identify protected files

Email options
PST
NSF
DBX
EDB
AOL
MBOX

Compound file options
Mount archive files

Index Options
Index text and metadata
Skip known files in hash library
Skip all files in hash library
Noise file:
Minimum word length: 3
Maximum word length: 64

Figure 7-12 Evidence Processor – Expand compound files

The processed compound files are in the **Records** view, where you can browse individual files under the **Archive** folder.

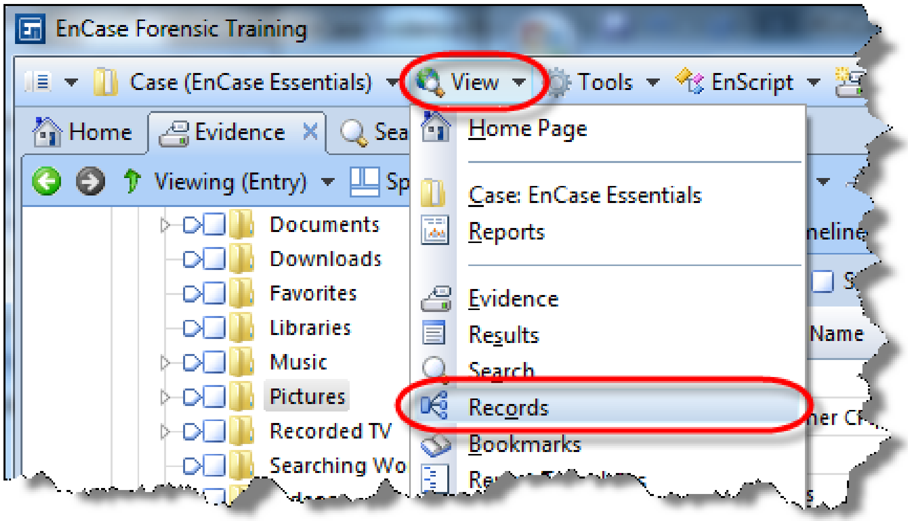


Figure 7-13 Records view

The way to search and view data across multiple archives is through a Search using an Index query and viewed through the **Search** tab.

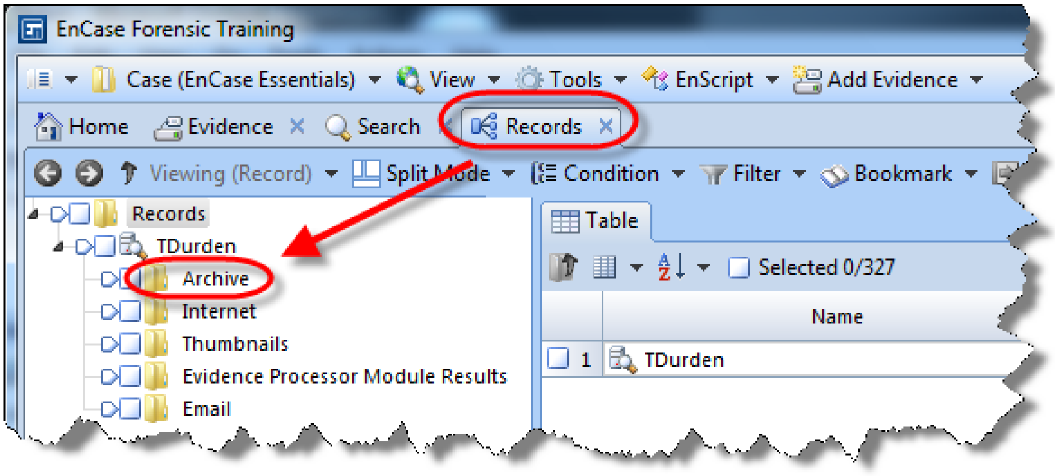
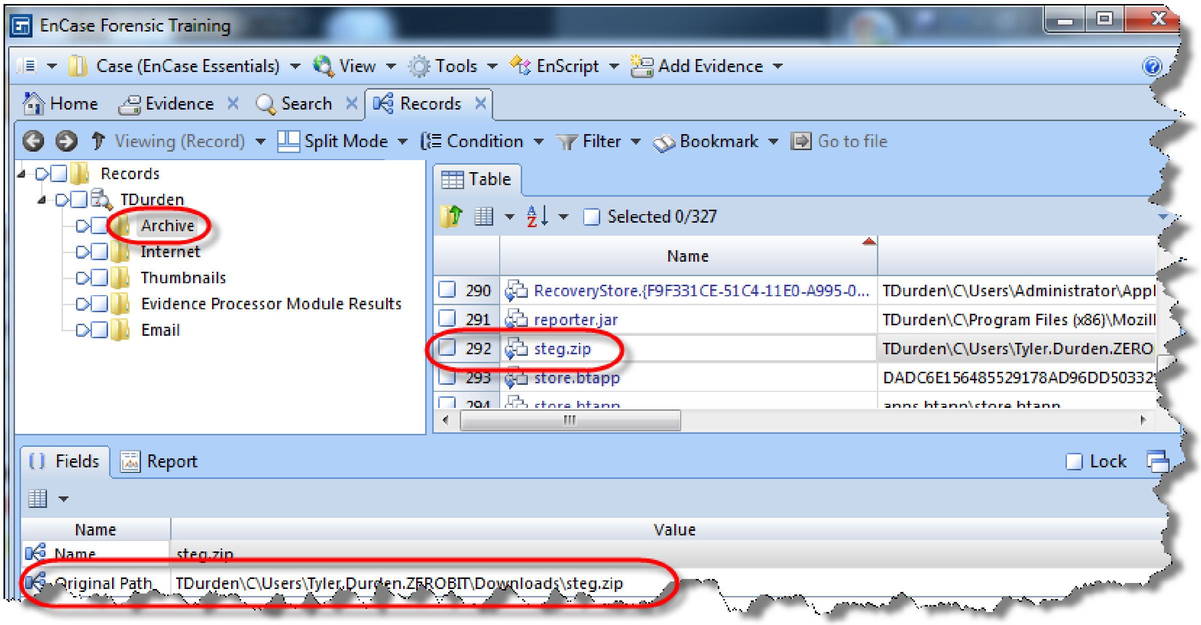


Figure 7-14 Records view – Archive folder

The compressed files are displayed under the **Archive** folder where they can be sorted and browsed for an examination. Click on the blue hyperlinked name of the archive to open it for review.

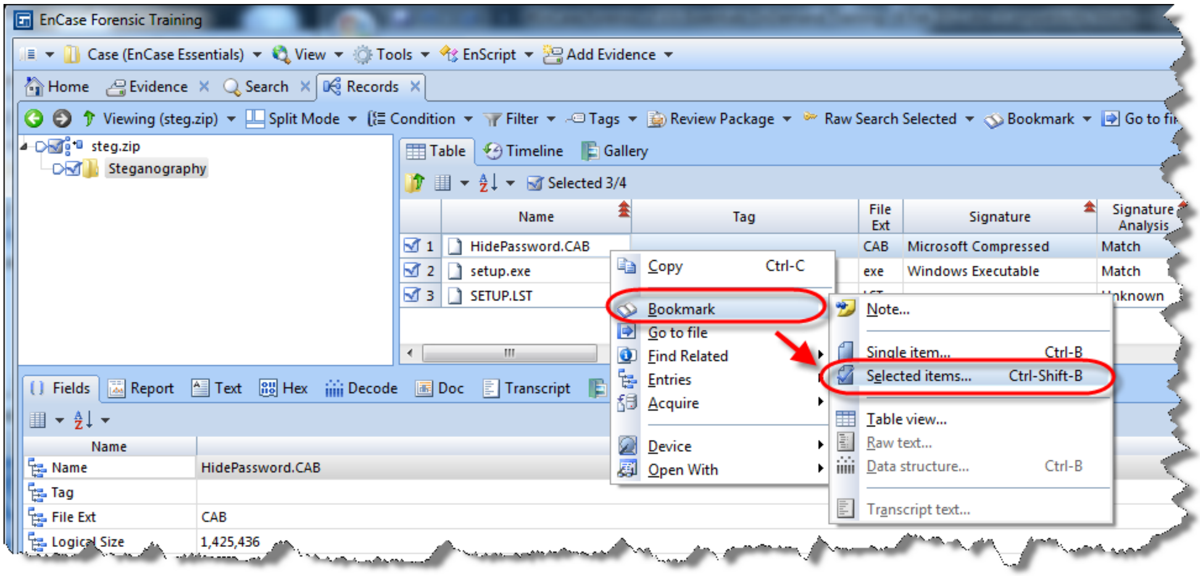

EnCase Forensic Training
Case (EnCase Essentials) View Tools EnScript Add Evidence
Home Evidence Search Records
Viewing (Record) Split Mode Condition Filter Bookmark Go to file
Records
TDurden
Archive
Internet
Thumbnails
Evidence Processor Module Results
Email
Table
Selected 0/327
Fields Report Lock

	Name	
290	RecoveryStore.{F9F331CE-51C4-11E0-A995-0...	TDurden\C\Users\Administrator\Appl
291	reporter.jar	TDurden\C\Program Files (x86)\Mozill
292	steg.zip	TDurden\C\Users\Tyler.Durden.ZERO
293	store.btapp	DADC6E156485529178AD96DD50332
294	store.btapp	apps.btapp\store.btapp

Name	Value
Name	steg.zip
Original Path	TDurden\C\Users\Tyler.Durden.ZEROBIT\Downloads\steg.zip

Figure 7-15 Archive folder

You can open the compound file and view the contents. In this case, it is a steganography program, which you may wish to Bookmark as relevant evidence.


EnCase Forensic Training
Case (EnCase Essentials) View Tools EnScript Add Evidence
Home Evidence Search Records
Viewing (steg.zip) Split Mode Condition Filter Tags Review Package Raw Search Selected Bookmark Go to fi
steg.zip
Steganography
Table Timeline Gallery
Selected 3/4
Fields Report Text Hex Decode Doc Transcript
Copy Ctrl-C
Bookmark
Go to file
Find Related
Entries
Acquire
Device
Open With
Note...
Single item... Ctrl-B
Selected items... Ctrl-Shift-B
Table view...
Raw text...
Data structure... Ctrl-B
Transcript text...

	Name	Tag	File Ext	Signature	Signature Analysis
1	HidePassword.CAB		CAB	Microsoft Compressed	Match
2	setup.exe		exe	Windows Executable	Match
3	SETUP.LST		LST		Unknown

Name	
Name	HidePassword.CAB
Tag	
File Ext	CAB
Logical Size	1,425,436

Figure 7-16 Browsing Archive file

Use the **Back** button to return to the **Record** view.

Internet Artifacts

To review the processed Internet artifacts, select the **Internet** folder in the Tree Pane and then the **Internet** hyperlink in the Table Pane.

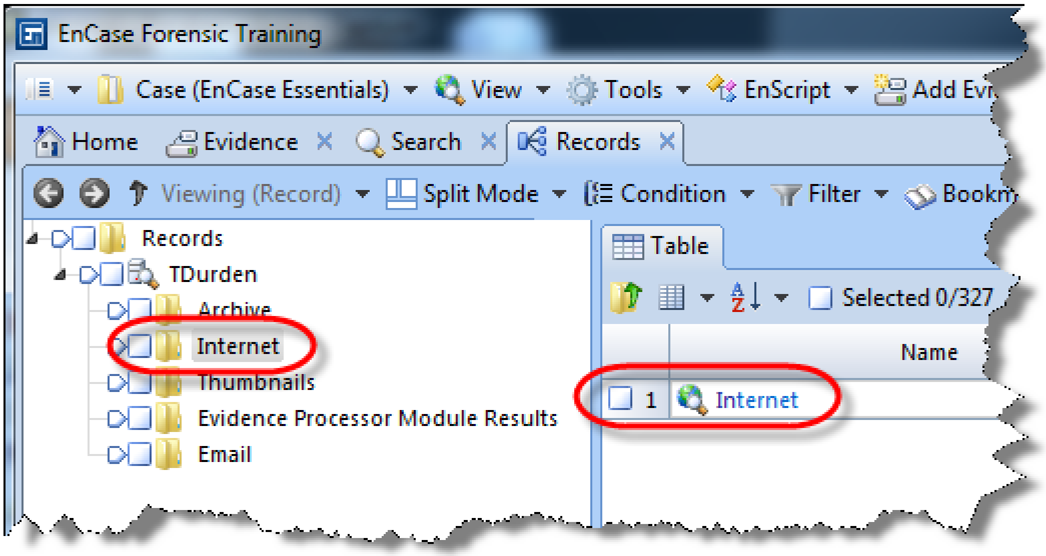
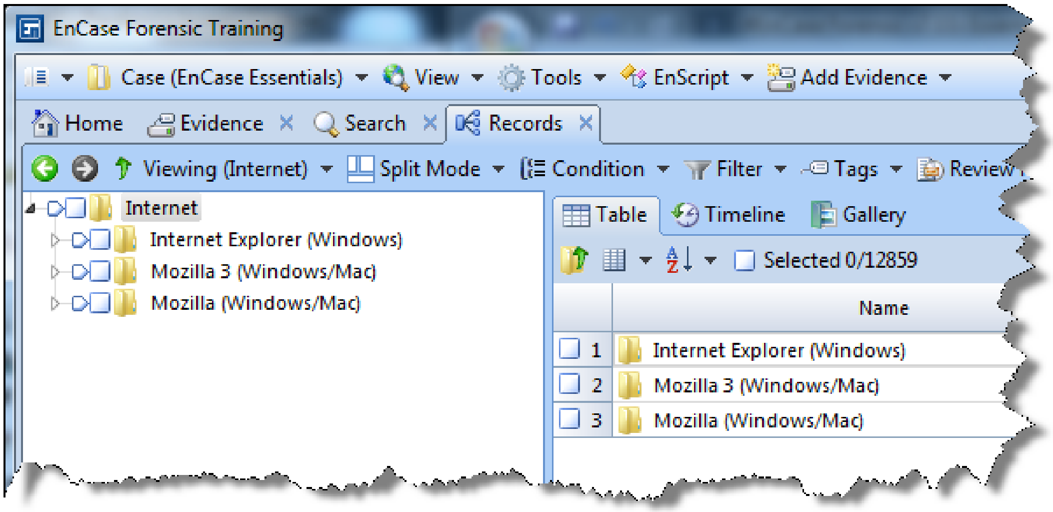


Figure 7-17 Accessing processed Internet artifacts

The Internet browsers with discovered and processed artifacts will be displayed in folders, such **Internet Explorer** and **Mozilla** as shown in the following figure. If applicable, those artifacts that are recovered and cannot be associated with a specific browser are placed in an **Unknown Browser** folder.



	Name
1	Internet Explorer (Windows)
2	Mozilla 3 (Windows/Mac)
3	Mozilla (Windows/Mac)

Figure 7-18 Internet artifacts organized by browser

Currently, six browsers are supported. They are:

- Internet Explorer
- Macintosh Internet Explorer
- Safari
- Firefox
- Opera
- Chrome

NOTE: The difference between a regular search for Internet artifacts and a search of Internet artifacts in the unallocated clusters, is that keywords are added internally and marked with a special tag indicating that it is for Internet history searching only.

Internet Explorer 9 Support

EnCase supports Internet Explorer 9 bookmarks, parsing all Internet Explorer 9 artifacts, including:

- Bookmarks
- Cookies
- Downloads
- Keyword searches
- History
- Login data
- Cache
- Visited links
- Web data

This gives you the option to search allocated or unallocated files for these Internet Explorer 9 artifacts. When processing is finished, you can also view and search inside Internet history items for these artifacts.

Google Chrome Internet Artifacts

EnCase v7 includes support for parsing these Google Chrome Internet artifacts:

Term	Definition
History	A list of Web sites recently visited. This typically consists of Web sites, usage, and time related data.
Cookies	A list of recent authentication and session data for sites with persistent usage. This typically consists of Web site, expiration times, and site-specific cookie data.
Cache	A list of recently cached files.
Downloads	A list of recently downloaded files, typically consisting of Web sites, file names, location, size, and date.
Keyword Search	A list of recent keyword searches. This typically consists of search terms and the search result page.
Login Data	A list of login data. This typically consists of Web sites, username, password, and SSL information.
Top Sites	A list of top Web sites such as Web site information, rank, thumbnails, and redirect information.

NOTE: EnCase does not currently provide the ability to recover Google Chrome Internet artifacts from unallocated clusters.

Firefox Artifacts

As an enhancement to the Search for Internet history function, EnCase parses Firefox artifacts stored in a SQLite database and displays them in the Records tab.

The types of Firefox 8 artifacts parsed are:

- Bookmarks
- Cookies
- Downloads
- Keyword Searches
- History
- Form Data
- Cache
- Visited Links
- Web Data

NOTE: The Records tab of an Internet history search for Mozilla Firefox artifacts displays Frecency and Rev Host Name columns.

- "Frecency" is a valid word used by Mozilla. Do not mistake it for "frequency." For more information, see the Mozilla developer center article at ***https://developer.mozilla.org/en/The_Places_frecency_algorithm***.
- The value displayed in the Frecency column is the score Mozilla gives to each URL. It includes how frequently a person visits the site and how recently the user visits the site. EnCase displays this value as it is stored in the places.sqlite file.
- Mozilla stores a URL's host name in reverse. EnCase displays it as such in the Rev Host Name column.

Enhanced Firefox 10 and IE 9 Browsing History Support

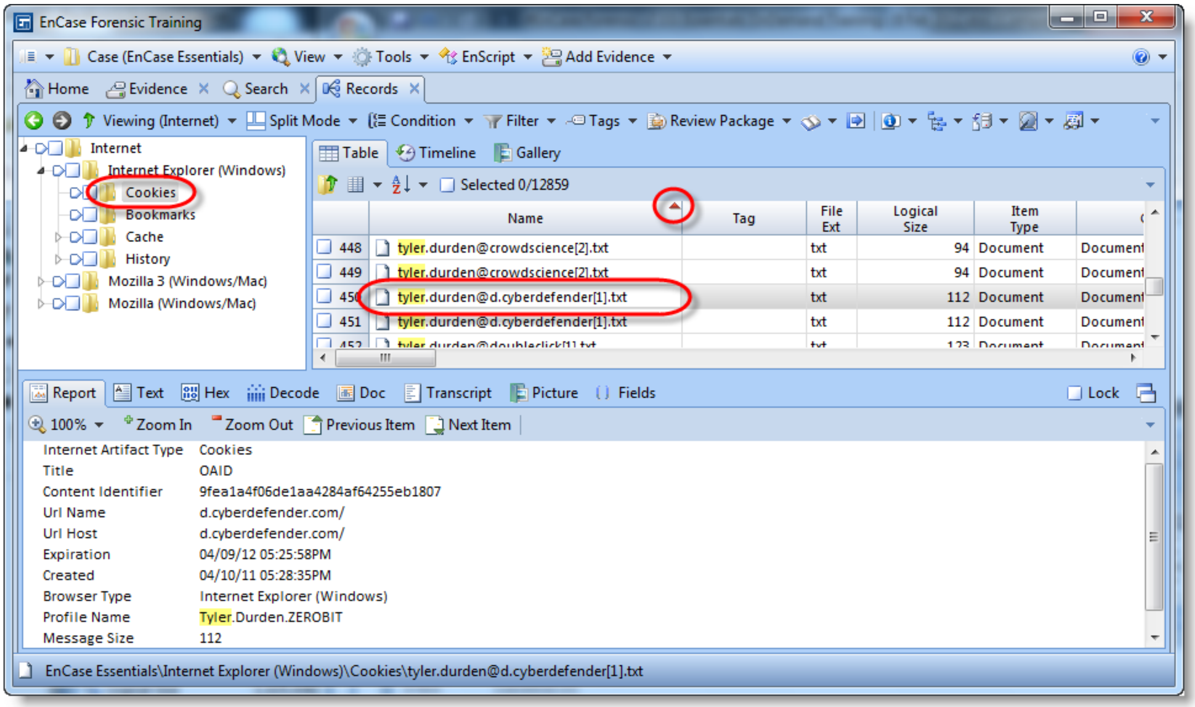
EnCase now recovers more browsing history from Firefox 10 and Internet Explorer 9. This provides up to three weeks of browsing history and can result in recovering thousands of cookies, downloads, bookmarks, and website visits. System time will not be changed to mimic the time span on the system being acquired to ensure valid data is recovered.

Analyzing the Internet Artifacts

The Internet artifacts are organized into categories. You can bookmark the relevant evidence found to be included within the report.

- **Cookies** – Text file stored on a hard drive by the web browser;may be used for authentication, shopping, preferences, etc.

  NOTE: You can sort on the Name column to make the examination more efficient.



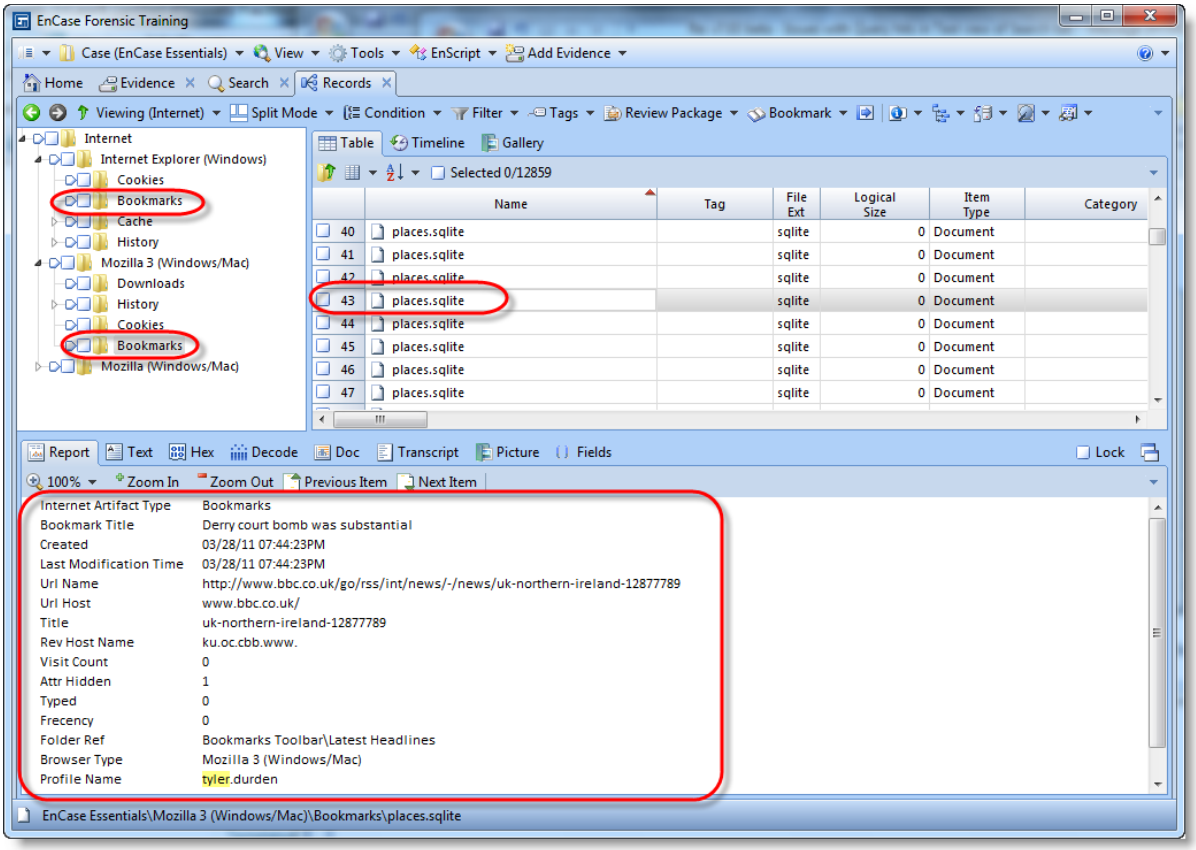
	Name	Tag	File Ext	Logical Size	Item Type	
448	tyler.durden@crowdscience[2].txt		txt	94	Document	Document
449	tyler.durden@crowdscience[2].txt		txt	94	Document	Document
450	tyler.durden@d.cyberdefender[1].txt		txt	112	Document	Document
451	tyler.durden@d.cyberdefender[1].txt		txt	112	Document	Document
452	tyler.durden@doubleclick[1].txt		txt	123	Document	Document

Internet Artifact Type	Cookies
Title	OAID
Content Identifier	9fea1a4f06de1aa4284af64255eb1807
Url Name	d.cyberdefender.com/
Url Host	d.cyberdefender.com/
Expiration	04/09/12 05:25:58PM
Created	04/10/11 05:28:35PM
Browser Type	Internet Explorer (Windows)
Profile Name	Tyler.Durden.ZEROBIT
Message Size	112

EnCase Essentials\Internet Explorer (Windows)\Cookies\tyler.durden@d.cyberdefender[1].txt

Figure 7-19 Internet cookies

- **Bookmarks** – Also known as "Favorites" or "Internet shortcuts"



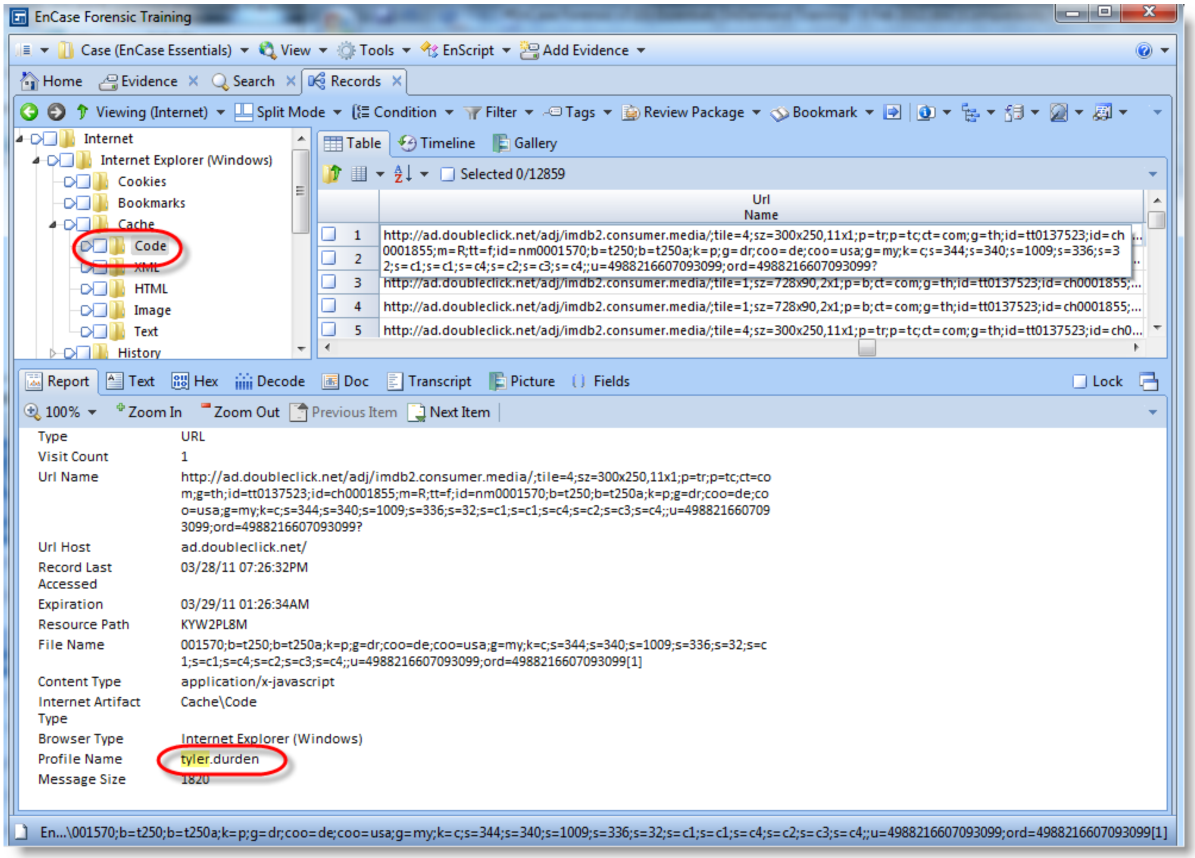
	Name	Tag	File Ext	Logical Size	Item Type	Category
40	places.sqlite		sqlite	0	Document	
41	places.sqlite		sqlite	0	Document	
42	places.sqlite		sqlite	0	Document	
43	places.sqlite		sqlite	0	Document	
44	places.sqlite		sqlite	0	Document	
45	places.sqlite		sqlite	0	Document	
46	places.sqlite		sqlite	0	Document	
47	places.sqlite		sqlite	0	Document	

Internet Artifact Type	Bookmarks
Bookmark Title	Derry court bomb was substantial
Created	03/28/11 07:44:23PM
Last Modification Time	03/28/11 07:44:23PM
Url Name	http://www.bbc.co.uk/go/rss/int/news/-/news/uk-northern-ireland-12877789
Url Host	www.bbc.co.uk/
Title	uk-northern-ireland-12877789
Rev Host Name	ku.oc.cbb.www.
Visit Count	0
Attr Hidden	1
Typed	0
Frecency	0
Folder Ref	Bookmarks Toolbar\Latest Headlines
Browser Type	Mozilla 3 (Windows/Mac)
Profile Name	tyler.durden

EnCase Essentials\Mozilla 3 (Windows/Mac)\Bookmarks\places.sqlite

Figure 7-20 Bookmarks – Internet Shortcut

- **Cache** – Files are written to the hard drive to increase the in loading speed of frequently visited web pages
    - **Code** – Downloaded code from visited websites, including animated GIFs



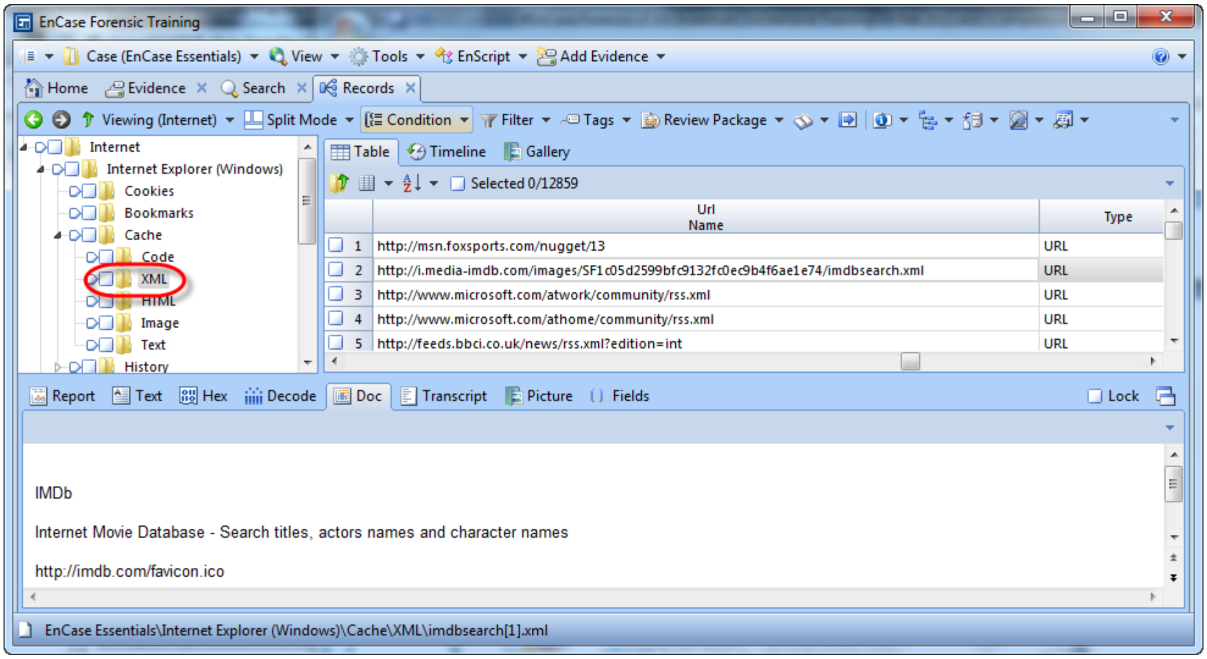
	Url Name
1	http://ad.doubleclick.net/adj/imdb2.consumer.media/;tile=4;sz=300x250,11x1;p=tr;p=tc;ct=com;g=th;id=tt0137523;id=ch0001855;m=R;tt=f;id=nm0001570;b=t250;b=t250a;k=p;g=dr;coo=de;coo=usa;g=my;k=c;s=344;s=340;s=1009;s=336;s=32;s=c1;s=c1;s=c4;s=c2;s=c3;s=c4;;u=4988216607093099;ord=4988216607093099?
2	
3	http://ad.doubleclick.net/adj/imdb2.consumer.media/;tile=1;sz=728x90,2x1;p=b;ct=com;g=th;id=tt0137523;id=ch0001855;...
4	http://ad.doubleclick.net/adj/imdb2.consumer.media/;tile=1;sz=728x90,2x1;p=b;ct=com;g=th;id=tt0137523;id=ch0001855;...
5	http://ad.doubleclick.net/adj/imdb2.consumer.media/;tile=4;sz=300x250,11x1;p=tr;p=tc;ct=com;g=th;id=tt0137523;id=ch0...

Type	URL
Visit Count	1
Url Name	http://ad.doubleclick.net/adj/imdb2.consumer.media/;tile=4;sz=300x250,11x1;p=tr;p=tc;ct=com;g=th;id=tt0137523;id=ch0001855;m=R;tt=f;id=nm0001570;b=t250;b=t250a;k=p;g=dr;coo=de;coo=usa;g=my;k=c;s=344;s=340;s=1009;s=336;s=32;s=c1;s=c1;s=c4;s=c2;s=c3;s=c4;;u=4988216607093099;ord=4988216607093099?
Url Host	ad.doubleclick.net/
Record Last Accessed	03/28/11 07:26:32PM
Expiration	03/29/11 01:26:34AM
Resource Path	KYW2PL8M
File Name	001570;b=t250;b=t250a;k=p;g=dr;coo=de;coo=usa;g=my;k=c;s=344;s=340;s=1009;s=336;s=32;s=c1;s=c1;s=c4;s=c2;s=c3;s=c4;;u=4988216607093099;ord=4988216607093099[1]
Content Type	application/x-javascript
Internet Artifact Type	Cache\Code
Browser Type	Internet Explorer (Windows)
Profile Name	tyler.durden
Message Size	1820

En...\001570;b=t250;b=t250a;k=p;g=dr;coo=de;coo=usa;g=my;k=c;s=344;s=340;s=1009;s=336;s=32;s=c1;s=c1;s=c4;s=c2;s=c3;s=c4;;u=4988216607093099;ord=4988216607093099[1]

Figure 7-21 Internet Cache – Code

- **XML** – Extensible Markup Language pages visited by the browser



	Url Name	Type
1	http://msn.foxsports.com/nugget/13	URL
2	http://i.media-imdb.com/images/SF1c05d2599bfc9132fc0ec9b4f6ae1e74/imdbsearch.xml	URL
3	http://www.microsoft.com/atwork/community/rss.xml	URL
4	http://www.microsoft.com/athome/community/rss.xml	URL
5	http://feeds.bbci.co.uk/news/rss.xml?edition=int	URL

IMDb

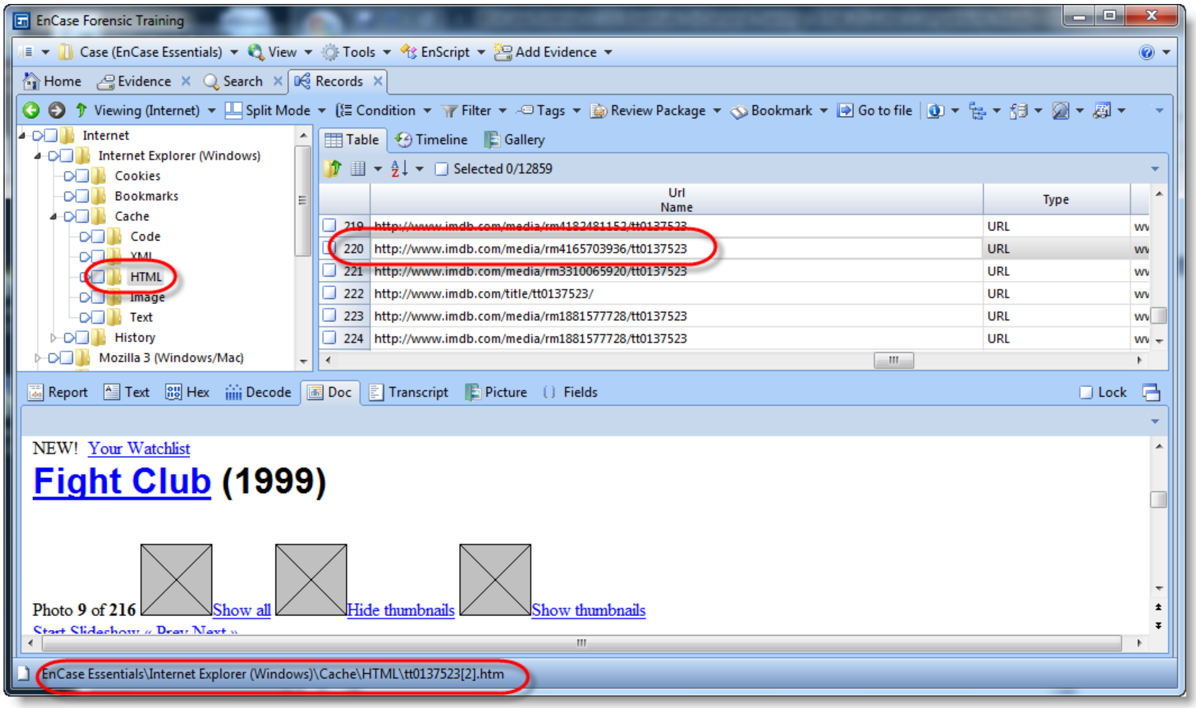
Internet Movie Database - Search titles, actors names and character names

http://imdb.com/favicon.ico

EnCase Essentials\Internet Explorer (Windows)\Cache\XML\imdbsearch[1].xml

Figure 7-22 Internet Cache – XML

- **HTML** – Hypertext Markup Language of visited web pages. Best viewed in the Doc view. Placeholders for images are depicted by the box with the "X."



	Url Name	Type	
219	http://www.imdb.com/media/rm4182481152/tt0137523	URL	wv
220	http://www.imdb.com/media/rm4165703936/tt0137523	URL	wv
221	http://www.imdb.com/media/rm3310065920/tt0137523	URL	wv
222	http://www.imdb.com/title/tt0137523/	URL	wv
223	http://www.imdb.com/media/rm1881577728/tt0137523	URL	wv
224	http://www.imdb.com/media/rm1881577728/tt0137523	URL	wv

NEW! Your Watchlist

Fight Club (1999)

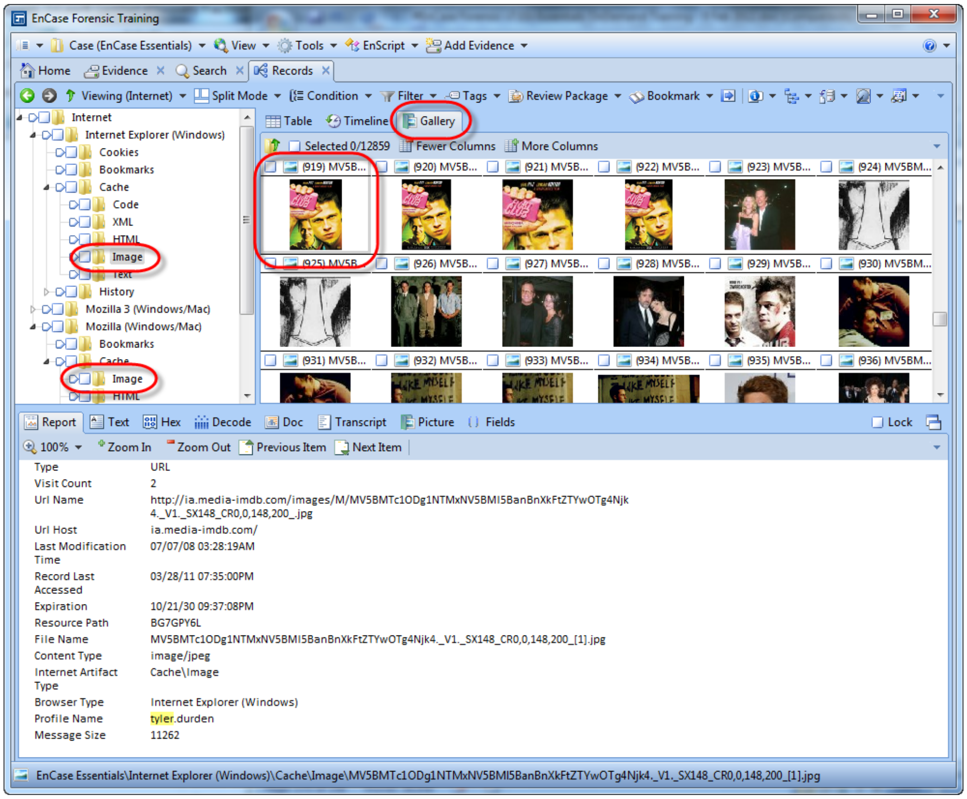
Photo 9 of 216 Show all Hide thumbnails Show thumbnails

Start Slideshow « Prev Next »

EnCase Essentials\Internet Explorer (Windows)\Cache\HTML\tt0137523[2].htm

Figure 7-23 Internet Cache – HTML

- **Image** – Best viewed in the Gallery view for quick review. The Timeline view will assist with tracking user activity; the Table view contains the URL (Uniform Recourse Link) of the source website and date/time stamps, also available in the Report tab of the Review Pane.

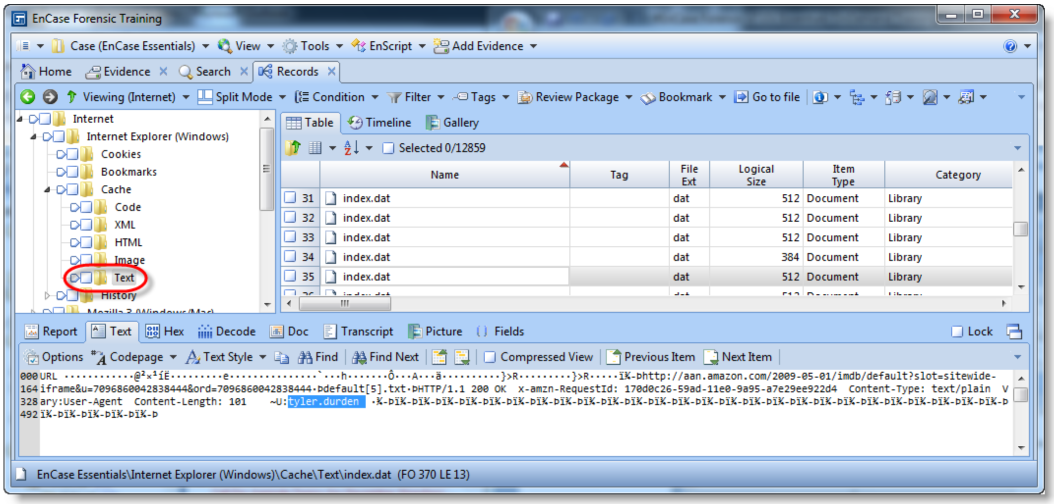


Type	URL
Visit Count	2
Url Name	http://ia.media-imdb.com/images/M/MV5BMTc1ODg1NTMxNV5BMl5BanBnXkFtZTYwOTg4Njk4._V1._SX148_CR0,0,148,200_.jpg
Url Host	ia.media-imdb.com/
Last Modification Time	07/07/08 03:28:19AM
Record Last Accessed	03/28/11 07:35:00PM
Expiration	10/21/30 09:37:08PM
Resource Path	BG7GPY6L
File Name	MV5BMTc1ODg1NTMxNV5BMl5BanBnXkFtZTYwOTg4Njk4._V1._SX148_CR0,0,148,200_[1].jpg
Content Type	image/jpeg
Internet Artifact Type	Cache\Image
Browser Type	Internet Explorer (Windows)
Profile Name	tyler.durden
Message Size	11262

EnCase Essentials\Internet Explorer (Windows)\Cache\Image\MV5BMTc1ODg1NTMxNV5BMl5BanBnXkFtZTYwOTg4Njk4._V1._SX148_CR0,0,148,200_[1].jpg

Figure 7-24 Internet Cache – Image →Gallery

- **Text** – Text from visited web pages



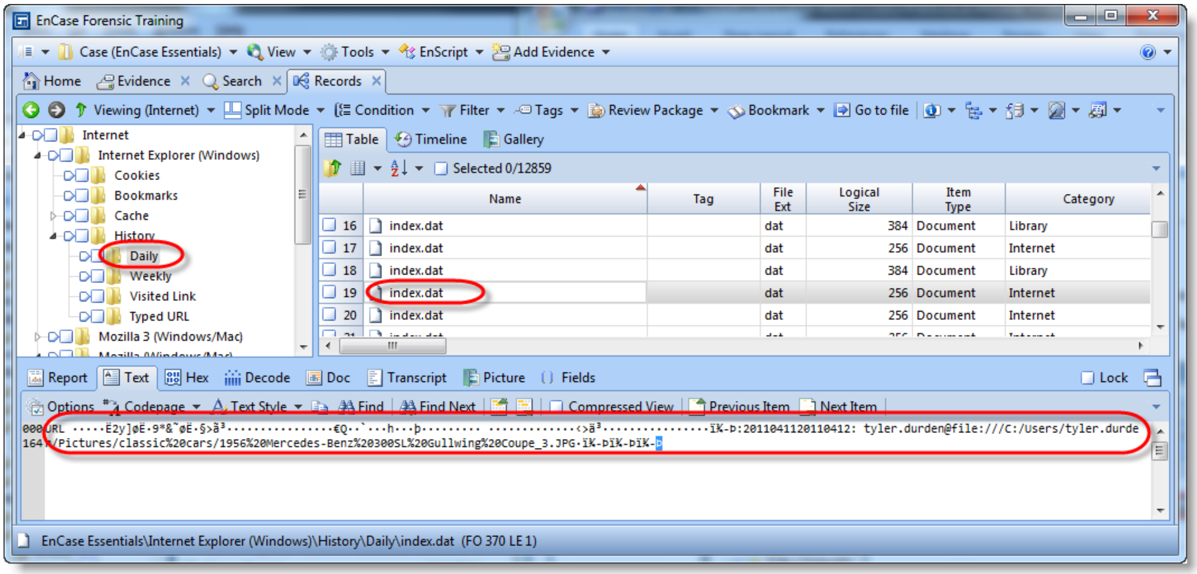
	Name	Tag	File Ext	Logical Size	Item Type	Category
31	index.dat		dat	512	Document	Library
32	index.dat		dat	512	Document	Library
33	index.dat		dat	512	Document	Library
34	index.dat		dat	384	Document	Library
35	index.dat		dat	512	Document	Library

```
000 URL ············@²×¹íË·········e···············`···h·······Ô···A···ã··········}>R·········}>R·····ïЖ-Þhttp://aan.amazon.com/2009-05-01/imdb/default?slot=sitewide-
164 iframe&u=7096860042838444&ord=7096860042838444·Þdefault[5].txt·ÞHTTP/1.1 200 OK  x-amzn-RequestId: 170d0c26-59ad-11e0-9a95-a7e29ee922d4  Content-Type: text/plain  V
328 ary:User-Agent  Content-Length: 101    ~U:tyler.durden  ·Ж-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-ÞïЖ-Þ
492 ïЖ-ÞïЖ-ÞïЖ-ÞïЖ-Þ
```

EnCase Essentials\Internet Explorer (Windows)\Cache\Text\index.dat (FO 370 LE 13)

Figure 7-25 Internet Cache – Text

- **History** – Record of the browsing through the web browser
  - **Daily History** – URLs from browsing as stored in the Daily History record, including Windows Explorer browsing by the user



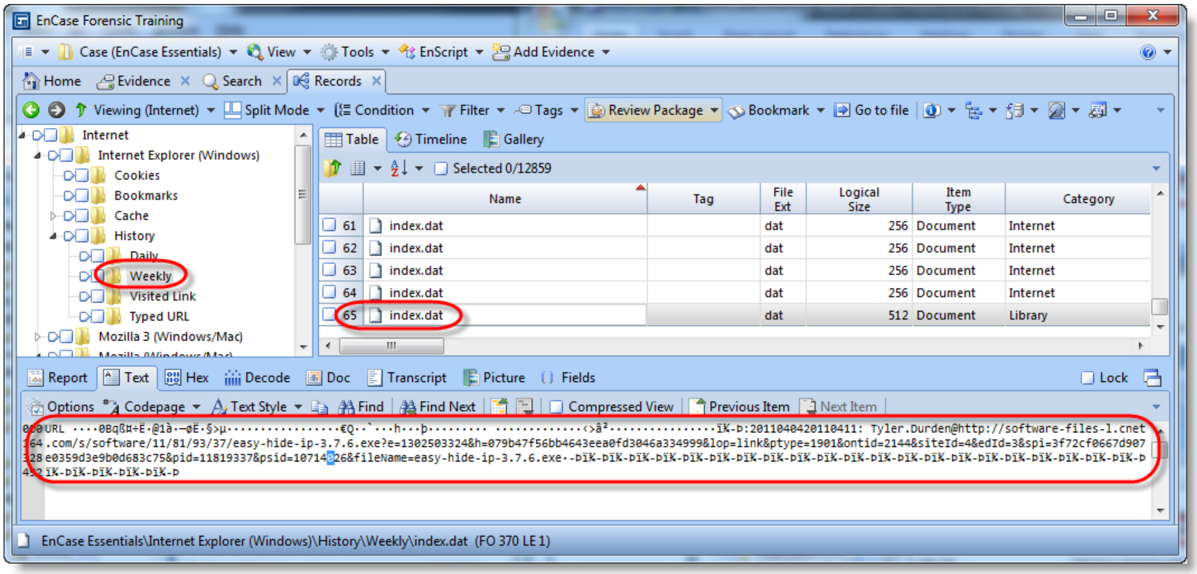
	Name	Tag	File Ext	Logical Size	Item Type	Category
16	index.dat		dat	384	Document	Library
17	index.dat		dat	256	Document	Internet
18	index.dat		dat	384	Document	Library
19	index.dat		dat	256	Document	Internet
20	index.dat		dat	256	Document	Internet

```
000 URL ·····Ë2y]øË·9*&˜øË·§>ã³················€Q··`···h···þ········ ·············‹>ã³················ï¾-Þ:2011041120110412: tyler.durden@file:///C:/Users/tyler.durde
164 /Pictures/classic%20cars/1956%20Mercedes-Benz%20300SL%20Gullwing%20Coupe_3.JPG·ï¾-Þï¾-Þï¾-Þ
```

EnCase Essentials\Internet Explorer (Windows)\History\Daily\index.dat (FO 370 LE 1)

Figure 7-26 Internet History – Daily History

  - **Weekly History** – URLs from browsing as stored in the Daily History record



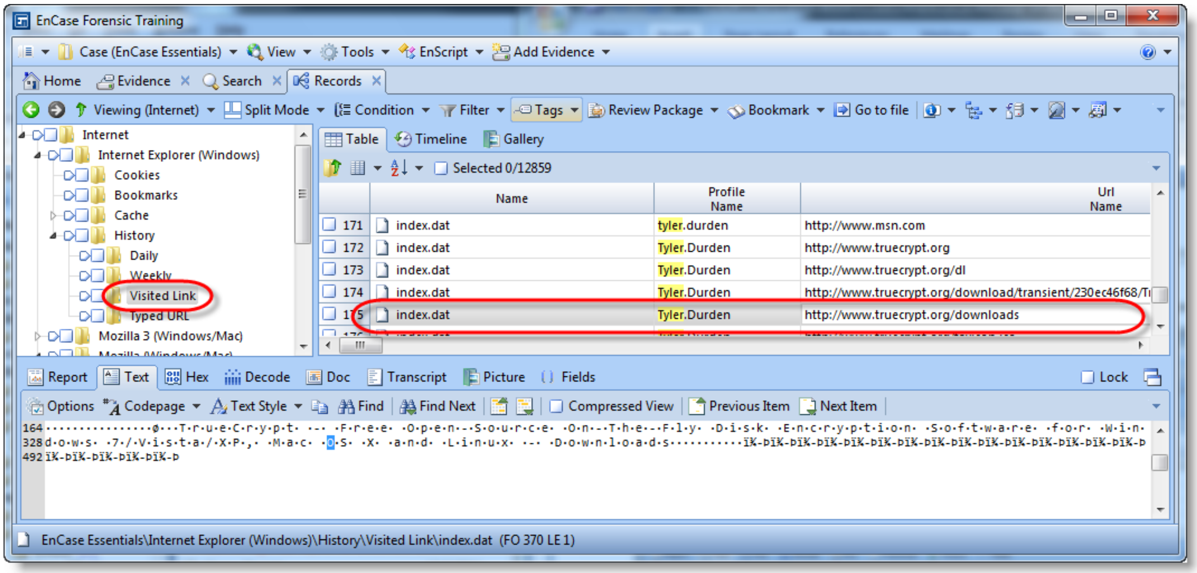
	Name	Tag	File Ext	Logical Size	Item Type	Category
61	index.dat		dat	256	Document	Internet
62	index.dat		dat	256	Document	Internet
63	index.dat		dat	256	Document	Internet
64	index.dat		dat	256	Document	Internet
65	index.dat		dat	512	Document	Library

```
000 URL ····0BqßÞ÷Ë·@1à·—øË·§>µ·················€Q··`···h···þ········ ·············‹>â²················ï¾-Þ:2011040420110411: Tyler.Durden@http://software-files-l.cnet
164 .com/s/software/11/81/93/37/easy-hide-ip-3.7.6.exe?e=1302503324&h=079b47f56bb4643eea0fd3046a334999&lop=link&ptype=1901&ontid=2144&siteId=4&edId=3&spi=3f72cf0667d907
328 e0359d3e9b0d683c75&pid=11819337&psid=10714026&fileName=easy-hide-ip-3.7.6.exe·-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þ
492 ï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þ
```

EnCase Essentials\Internet Explorer (Windows)\History\Weekly\index.dat (FO 370 LE 1)

Figure 7-27 Internet History – Weekly History

- ○ **Visited Link** – Website URL (Uniform Recourse Link) visited by browser



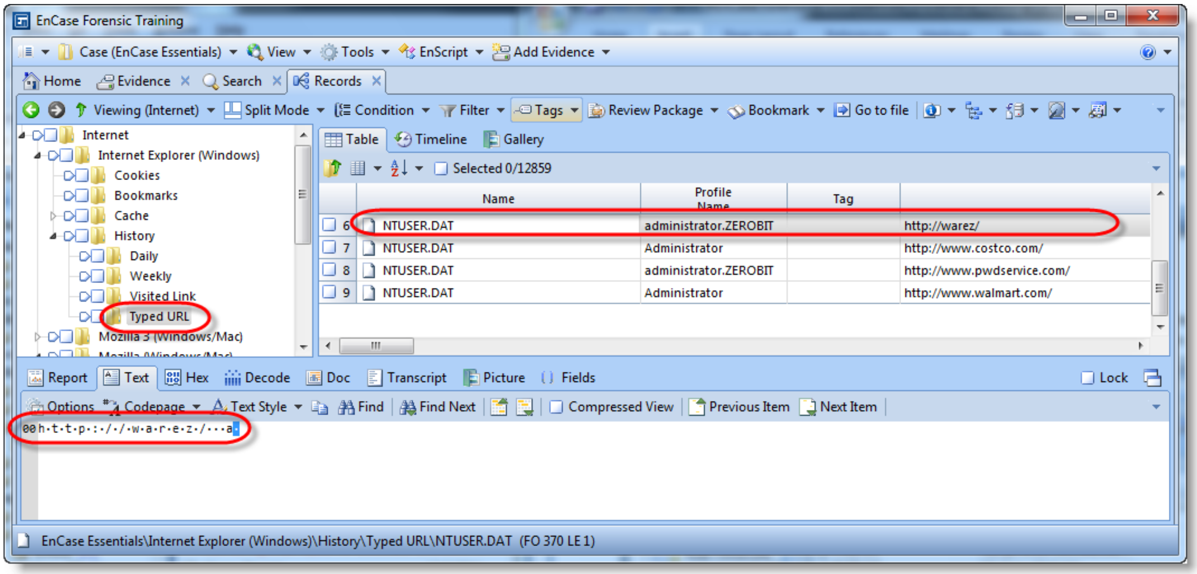
	Name	Profile Name	Url Name
171	index.dat	tyler.durden	http://www.msn.com
172	index.dat	Tyler.Durden	http://www.truecrypt.org
173	index.dat	Tyler.Durden	http://www.truecrypt.org/dl
174	index.dat	Tyler.Durden	http://www.truecrypt.org/download/transient/230ec46f68/Tı
175	index.dat	Tyler.Durden	http://www.truecrypt.org/downloads

```
164 ···············ø···T·r·u·e·C·r·y·p·t· ·-· ·F·r·e·e· ·O·p·e·n·-·S·o·u·r·c·e· ·O·n·-·T·h·e·-·F·l·y· ·D·i·s·k· ·E·n·c·r·y·p·t·i·o·n· ·S·o·f·t·w·a·r·e· ·f·o·r· ·W·i·n·
328 d·o·w·s· ·7·/·V·i·s·t·a·/·X·P·,· ·M·a·c· ·O·S· ·X· ·a·n·d· ·L·i·n·u·x· ·-· ·D·o·w·n·l·o·a·d·s··········ïӼ-ÞïӼ-ÞïӼ-ÞïӼ-ÞïӼ-ÞïӼ-ÞïӼ-ÞïӼ-ÞïӼ-ÞïӼ-ÞïӼ-ÞïӼ-ÞïӼ-ÞïӼ-Þ
492 ïӼ-ÞïӼ-ÞïӼ-ÞïӼ-ÞïӼ-Þ
```

EnCase Essentials\Internet Explorer (Windows)\History\Visited Link\index.dat (FO 370 LE 1)

Figure 7-28 Internet History – Visited Link

- ○ **Typed URL** – URLs typed directly into the browser by the user as stored in the user's NTUSER.DAT registry type. This is strong evidence of a deliberate act by the user.



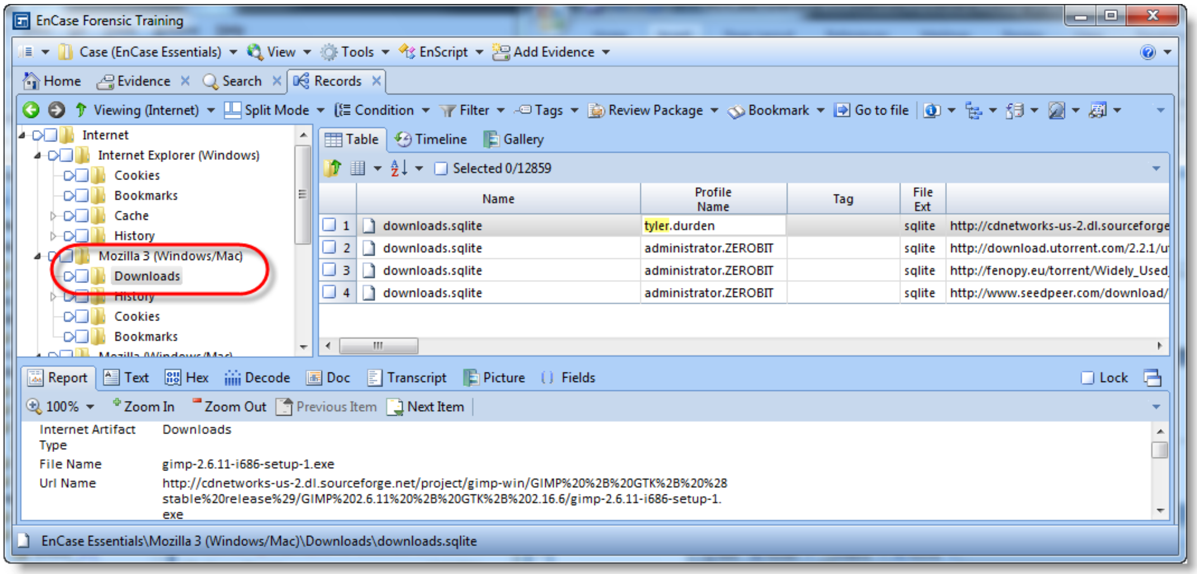
	Name	Profile Name	Tag	
6	NTUSER.DAT	administrator.ZEROBIT		http://warez/
7	NTUSER.DAT	Administrator		http://www.costco.com/
8	NTUSER.DAT	administrator.ZEROBIT		http://www.pwdservice.com/
9	NTUSER.DAT	Administrator		http://www.walmart.com/

```
00 h·t·t·p·:·/·/·w·a·r·e·z·/···a·
```

EnCase Essentials\Internet Explorer (Windows)\History\Typed URL\NTUSER.DAT (FO 370 LE 1)

Figure 7-29 Internet History – Typed URL

- **Downloads (Mozilla)** – Files downloaded via the browser



	Name	Profile Name	Tag	File Ext	
1	downloads.sqlite	tyler.durden		sqlite	http://cdnetworks-us-2.dl.sourceforge
2	downloads.sqlite	administrator.ZEROBIT		sqlite	http://download.utorrent.com/2.2.1/u
3	downloads.sqlite	administrator.ZEROBIT		sqlite	http://fenopy.eu/torrent/Widely_Used
4	downloads.sqlite	administrator.ZEROBIT		sqlite	http://www.seedpeer.com/download/

Internet Artifact Type Downloads
File Name gimp-2.6.11-i686-setup-1.exe
Url Name http://cdnetworks-us-2.dl.sourceforge.net/project/gimp-win/GIMP%20%2B%20GTK%2B%20%28stable%20release%29/GIMP%202.6.11%20%2B%20GTK%2B%202.16.6/gimp-2.6.11-i686-setup-1.exe

EnCase Essentials\Mozilla 3 (Windows/Mac)\Downloads\downloads.sqlite

Figure 7-30 Internet artifacts – Downloads

Use the **Back** button to return to the Records view

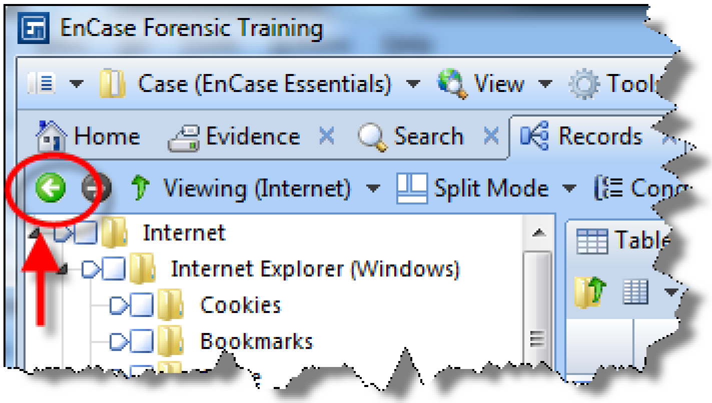


Figure 7-31 Back to Records

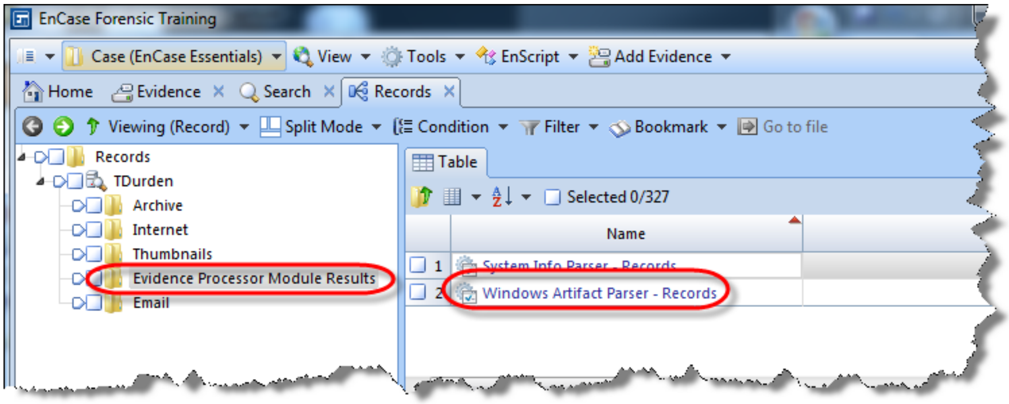
Evidence Processor Modules

The results of the Evidence Processor modules are also under the Records tab. Select the **Evidence Processor Module Results**.

The results are divided into categories:

- **Entries** – Files and folders on the file system
- **Records** – Evidence extracted, such as registry entries, link files, etc.

Click on the hyperlinked name to examine the results.

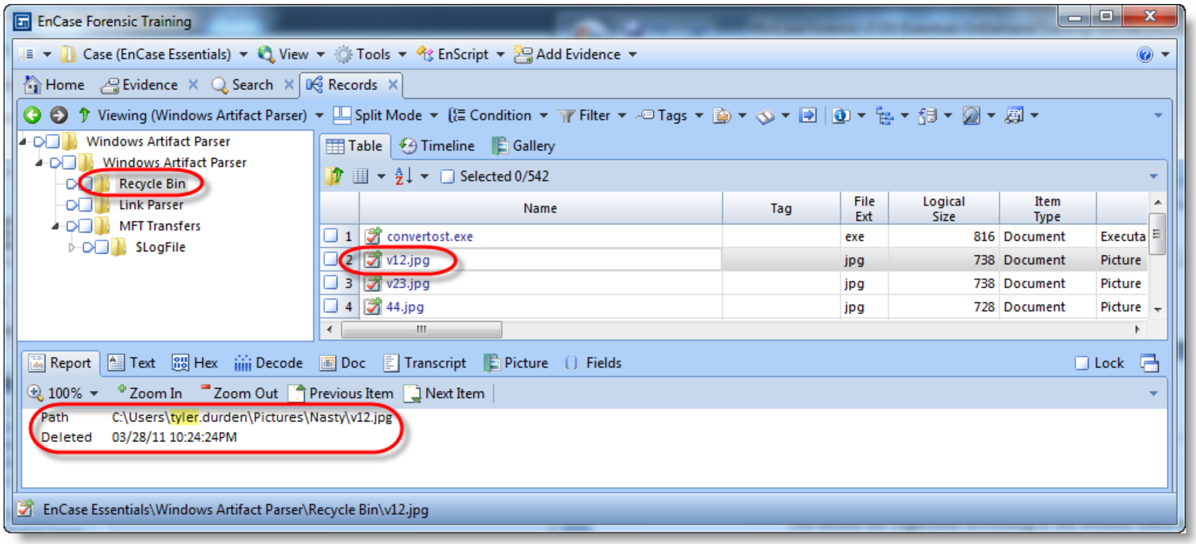


	Name
1	System Info Parser - Records
2	Windows Artifact Parser - Records

Figure 7-32 Evidence Processor Modules

Results – Modules

The results are organized according to the module name as shown in the following screenshot of a deleted image in the Recycle Bin.



	Name	Tag	File Ext	Logical Size	Item Type	
1	convertost.exe		exe	816	Document	Executa
2	v12.jpg		jpg	738	Document	Picture
3	v23.jpg		jpg	738	Document	Picture
4	44.jpg		jpg	728	Document	Picture

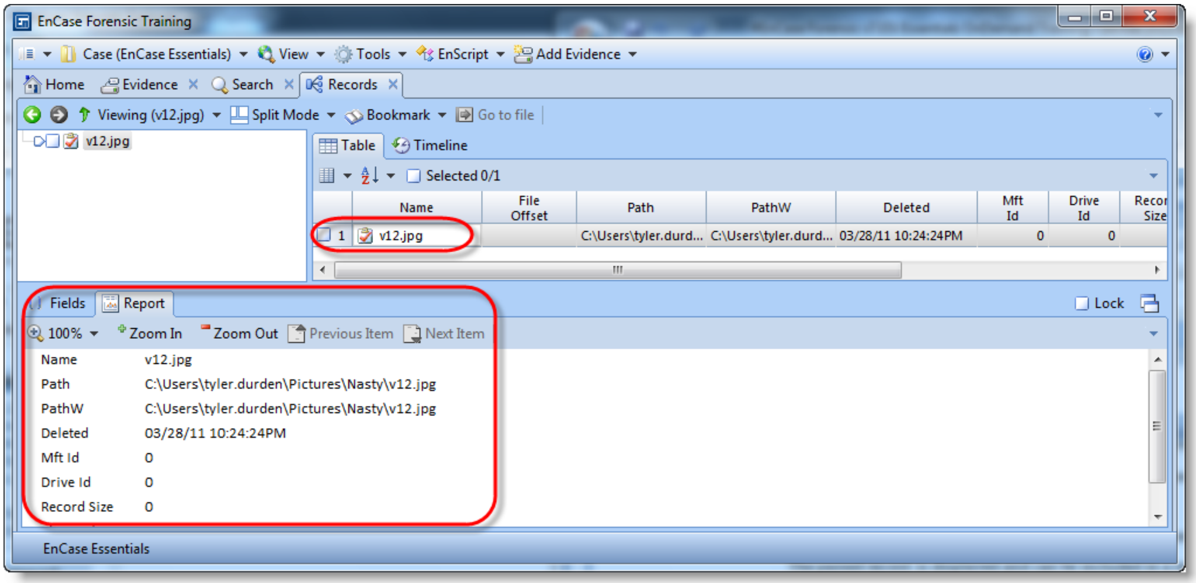
Path C:\Users\tyler.durden\Pictures\Nasty\v12.jpg
Deleted 03/28/11 10:24:24PM

EnCase Essentials\Windows Artifact Parser\Recycle Bin\v12.jpg

Figure 7-33 Windows Artifacts Parser

Click on the hyperlinked name to examine the multidimensional data, such as **V12.jpg**.

The parsed record is displayed and can be included in a report as a bookmark.



	Name	File Offset	Path	PathW	Deleted	Mft Id	Drive Id	Recor Size
1	v12.jpg		C:\Users\tyler.durd...	C:\Users\tyler.durd...	03/28/11 10:24:24PM	0	0	

Name	v12.jpg
Path	C:\Users\tyler.durden\Pictures\Nasty\v12.jpg
PathW	C:\Users\tyler.durden\Pictures\Nasty\v12.jpg
Deleted	03/28/11 10:24:24PM
Mft Id	0
Drive Id	0
Record Size	0

Figure 7-34 Parsed Recycle Bin record

Use the **Back** button to return to the Evidence Processor Module results.

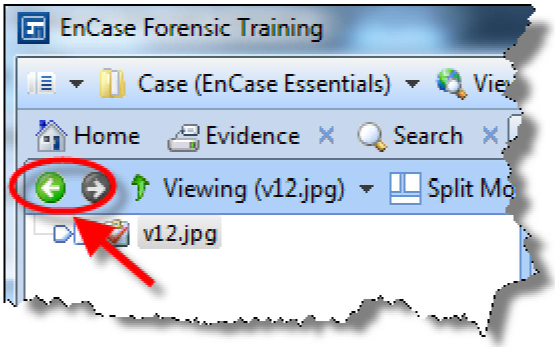
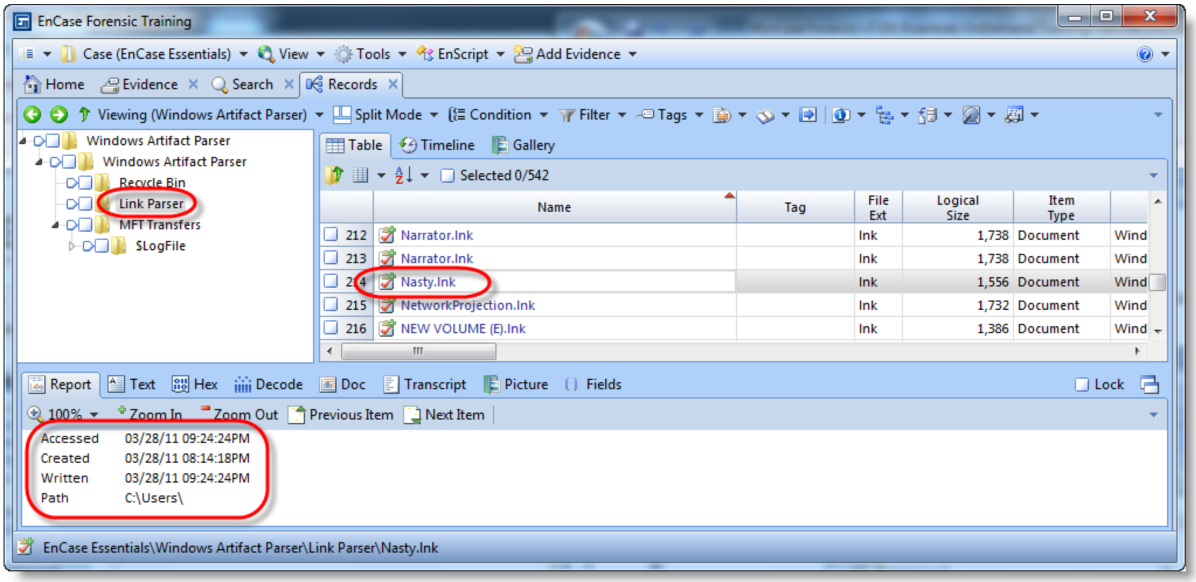


Figure 7-35 Back to Results

The Windows Artifact Parser includes other artifacts, such as the Link Parser.

Click on the name to view the parsed link file.



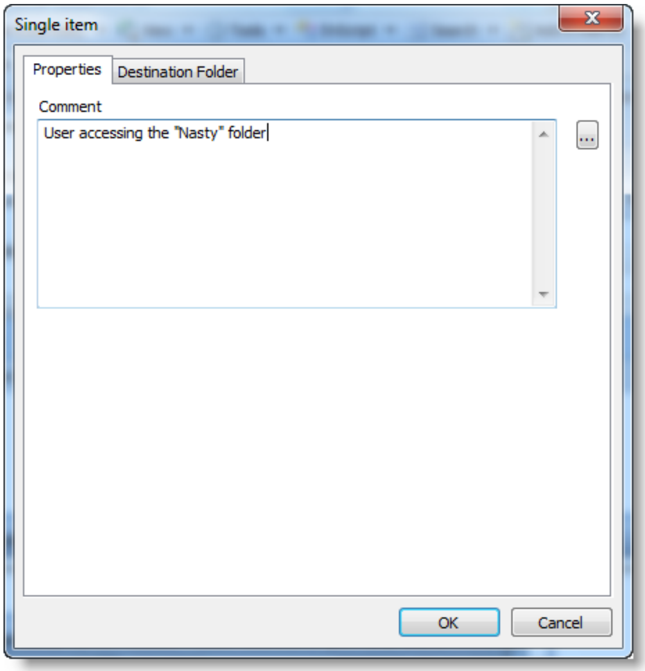
	Name	Tag	File Ext	Logical Size	Item Type	
212	Narrator.lnk		lnk	1,738	Document	Wind
213	Narrator.lnk		lnk	1,738	Document	Wind
214	Nasty.lnk		lnk	1,556	Document	Wind
215	NetworkProjection.lnk		lnk	1,732	Document	Wind
216	NEW VOLUME (E).lnk		lnk	1,386	Document	Wind

Accessed	03/28/11 09:24:24PM
Created	03/28/11 08:14:18PM
Written	03/28/11 09:24:24PM
Path	C:\Users\

EnCase Essentials\Windows Artifact Parser\Link Parser\Nasty.lnk

Figure 7-36 Link Parser

You can bookmark relevant evidence, such as the user accessing the Nasty folder containing previously bookmarked evidence items.



Comment

User accessing the "Nasty" folder

Figure 7-37 Bookmark comments

Place the bookmark into the appropriate Destination Folder.

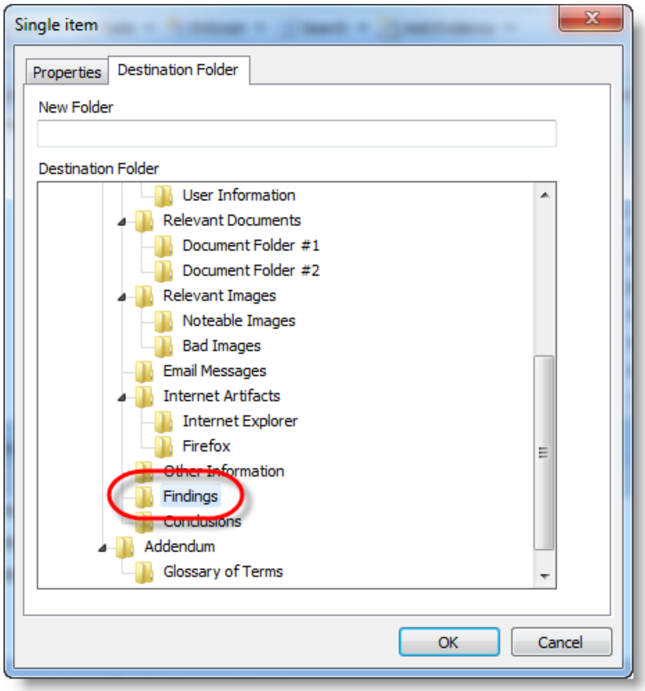


Figure 7-38 Bookmark Destination Folder

Creating a Hash Set

Hash sets (which contain the individual hash entries) are located within hash libraries. There are two steps to creating a hash set. The first step is to create an empty hash set within a library, and the second is to add information to it. To create a hash, you perform the following steps:

1. Click **Tools→Manage Hash Library**

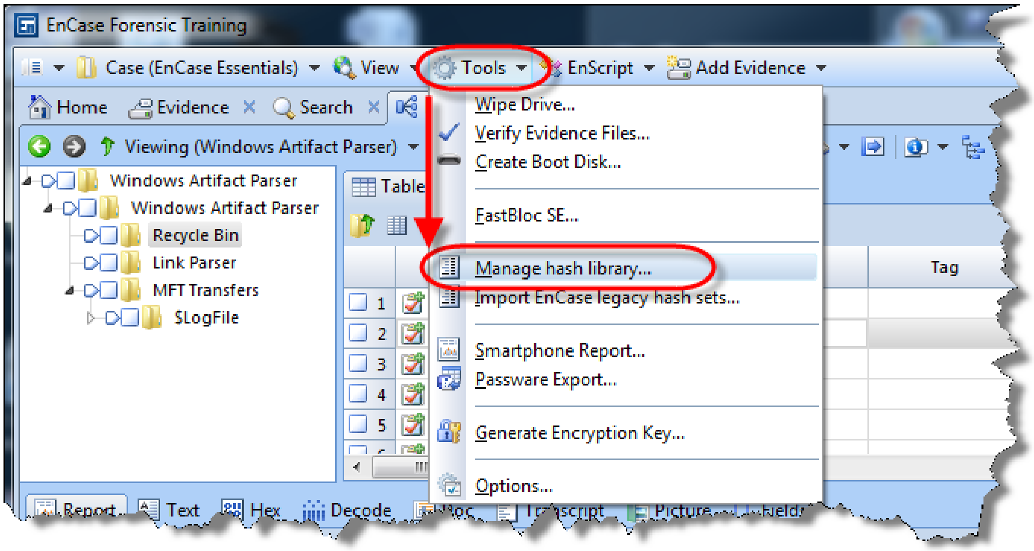
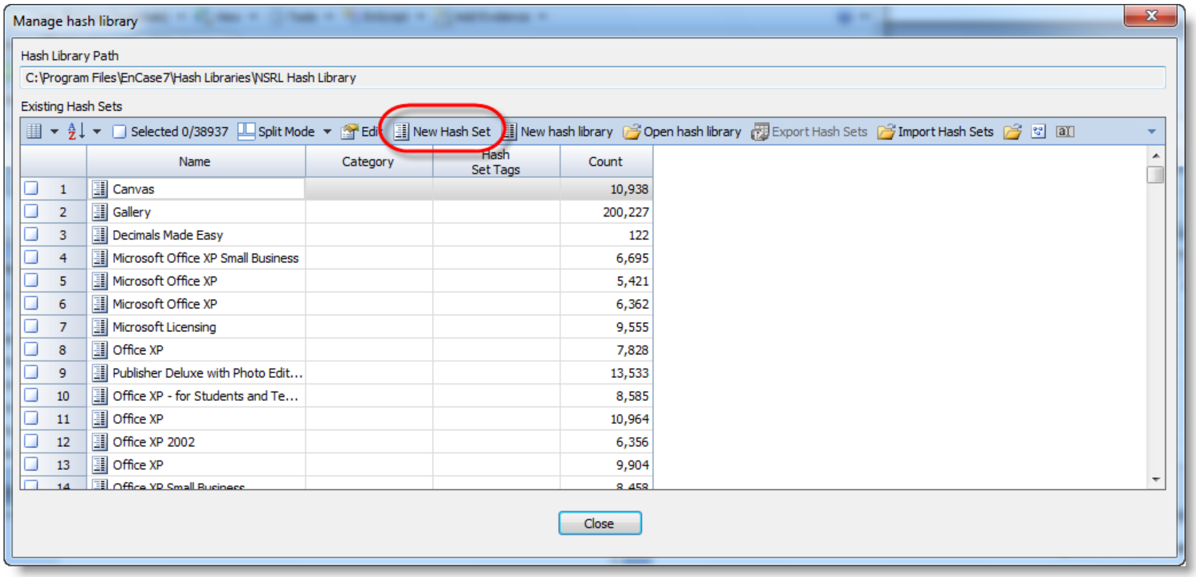


Figure 7-39 Manage Hash Library…

2. Make sure that you either browse and point to an existing hash library or create a new one (this is the hash library to which you will add the hash set)

3. On the Manage Hash Library panel toolbar, click **New Hash Set**



Hash Library Path

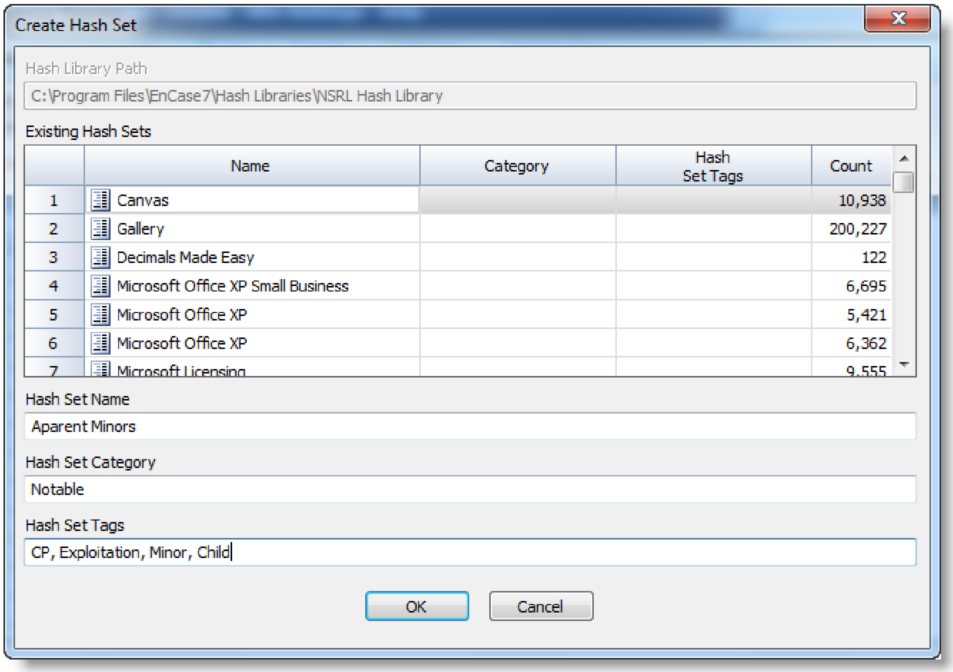
C:\Program Files\EnCase7\Hash Libraries\NSRL Hash Library

Existing Hash Sets

	Name	Category	Hash Set Tags	Count
☐ 1	Canvas			10,938
☐ 2	Gallery			200,227
☐ 3	Decimals Made Easy			122
☐ 4	Microsoft Office XP Small Business			6,695
☐ 5	Microsoft Office XP			5,421
☐ 6	Microsoft Office XP			6,362
☐ 7	Microsoft Licensing			9,555
☐ 8	Office XP			7,828
☐ 9	Publisher Deluxe with Photo Edit...			13,533
☐ 10	Office XP - for Students and Te...			8,585
☐ 11	Office XP			10,964
☐ 12	Office XP 2002			6,356
☐ 13	Office XP			9,904
☐ 14	Office XP Small Business			8,458

Figure 7-40 New Hash Set

4. Enter a Hash Set Name and information for Hash Set Category and Hash Set Tags



Hash Library Path

C:\Program Files\EnCase7\Hash Libraries\NSRL Hash Library

Existing Hash Sets

	Name	Category	Hash Set Tags	Count
1	Canvas			10,938
2	Gallery			200,227
3	Decimals Made Easy			122
4	Microsoft Office XP Small Business			6,695
5	Microsoft Office XP			5,421
6	Microsoft Office XP			6,362
7	Microsoft Licensing			9,555

Hash Set Name

Aparent Minors

Hash Set Category

Notable

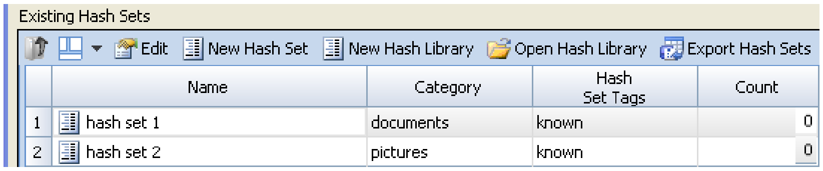
Hash Set Tags

CP, Exploitation, Minor, Child

Figure 7-41 Enter specific set information

5. Click **OK** and click **OK** again when you are prompted to add the new hash set.

The new hash set is listed under **Existing Hash Sets** in the Manage Hash Library panel.



Existing Hash Sets

	Name	Category	Hash Set Tags	Count
1	hash set 1	documents	known	0
2	hash set 2	pictures	known	0

Figure 7-42 Newly created hash set

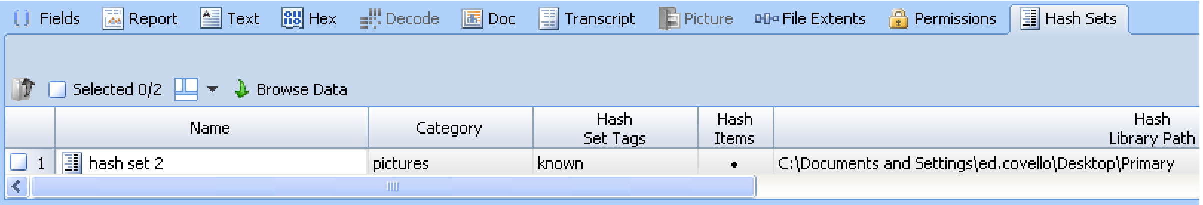
Adding Hash Values to a Hash Set

Once you have created a hash set within a library, you can add information to it. The steps for adding hash values to a hash set are as follows:

1. Add the device or evidence from which you want to generate a hash value to a case
2. Hash the files on the device by using the hashing feature of the Evidence Processor
3. Go to the table of evidence files or images whose hashes you want to add to the hash set
4. On the **Evidence** tab under the **Entries** table, expand the **Entries** view
5. In the **Table** tab, check those entries whose hash values you want to add to the hash set
6. In the Tab toolbar, click the **Entries** drop-down menu (indicated by a red arrow), and select **Add to Hash Library...**
   - The Add to Hash Library Panel displays
7. Choose the Hash Library to which to add the hash items by using the **Hash Library Type** drop-down menu
   - Select the **Primary** or **Secondary** hash library if they are defined or you can select **Other** and browse to a library
8. Once you have selected a library, select one or more previously created hash sets from the **Existing Hash Sets** window
9. On the Add to Hash Library panel Fields list, select the fields you want to add to the hash library for the selected items
   - Some fields are added by default, however, you can add other optional fields, depending on your needs
   - All fields that are added to the set will be reported when a hash comparison matches a particular hash set; the more fields that you add to a set, the larger the set becomes
10. Click **OK**

11. If the hash values were added to a library that was set as the Primary or Secondary hash library, you can check whether the item was successfully added to the hash set as follows:

    - On the Table tab, highlight the row containing the item
    - In the bottom pane, click **Hash Sets**; the hash set name, hash library, and other hashing information about the item should appear



	Name	Category	Hash Set Tags	Hash Items	Hash Library Path
□ 1	hash set 2	pictures	known	•	C:\Documents and Settings\ed.covello\Desktop\Primary

Figure 7-43 Hash set details displayed

Notes

Notes

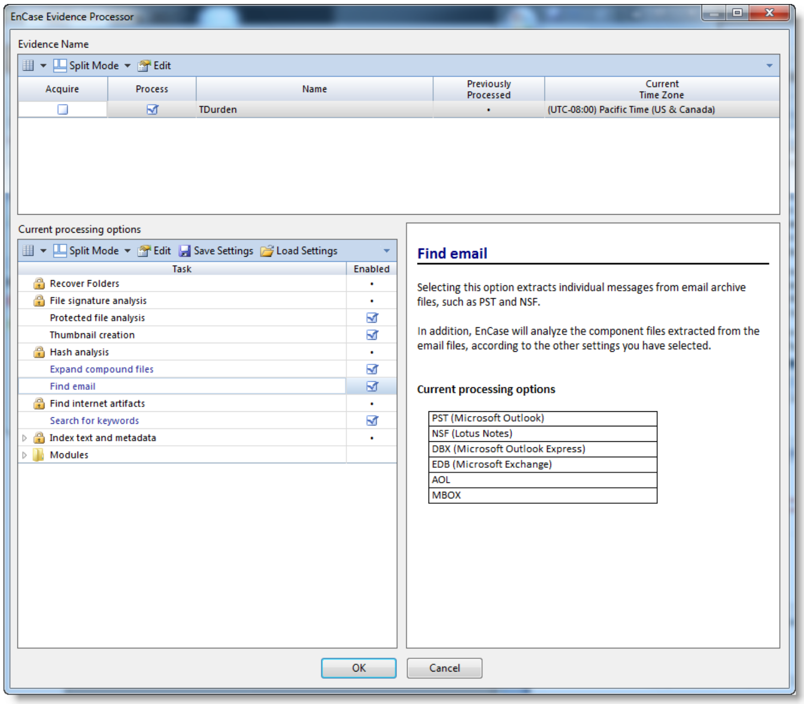
E-mail Results

E-mail is a key area for forensic investigation; it not only maintains a record of individual and corporate communications, but also contains date stamps, provides additional names or corporate entities, and may contain attachments. All of which can add to an investigation and supply further leads.

When e-mail is viewed in a case, EnCase® v7 can search for specific kinds of mail and parse its contents for examination. EnCase v7 lets you view e-mail in a format that is similar to common e-mail programs (for example, the Microsoft Office Outlook client). The views are customizable (you can view the data in tree, table, or composite views), allowing you to see only the data you want in the format you find most convenient.

EnCase v7 also allows you to track e-mail threads. In most situations, thread tracking can span multiple e-mail repositories, simplifying investigations that were previously complex and time-consuming. You use the **Find related – Show conversation** (e-mail thread) and **Find related – Show related messages** to view e-mails across multiple repositories.

Before conducting your e-mail analysis, make sure that you have already processed your case data with the Evidence Processor **Find email** selection checked.



Acquire	Process	Name	Previously Processed	Current Time Zone
□	☑	TDurden	•	(UTC-08:00) Pacific Time (US & Canada)

Task	Enabled
Recover Folders	•
File signature analysis	•
Protected file analysis	☑
Thumbnail creation	☑
Hash analysis	•
Expand compound files	☑
Find email	☑
Find internet artifacts	•
Search for keywords	☑
Index text and metadata	•
Modules	

Find email

Selecting this option extracts individual messages from email archive files, such as PST and NSF.

In addition, EnCase will analyze the component files extracted from the email files, according to the other settings you have selected.

Current processing options

PST (Microsoft Outlook)
NSF (Lotus Notes)
DBX (Microsoft Outlook Express)
EDB (Microsoft Exchange)
AOL
MBOX

Figure 8-1 Find e-mail

The processed e-mail will be found under the **Records** view.

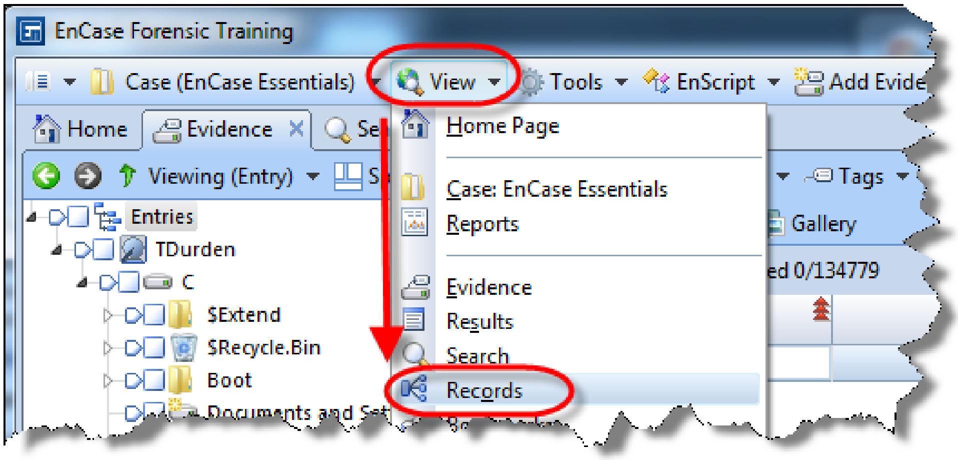
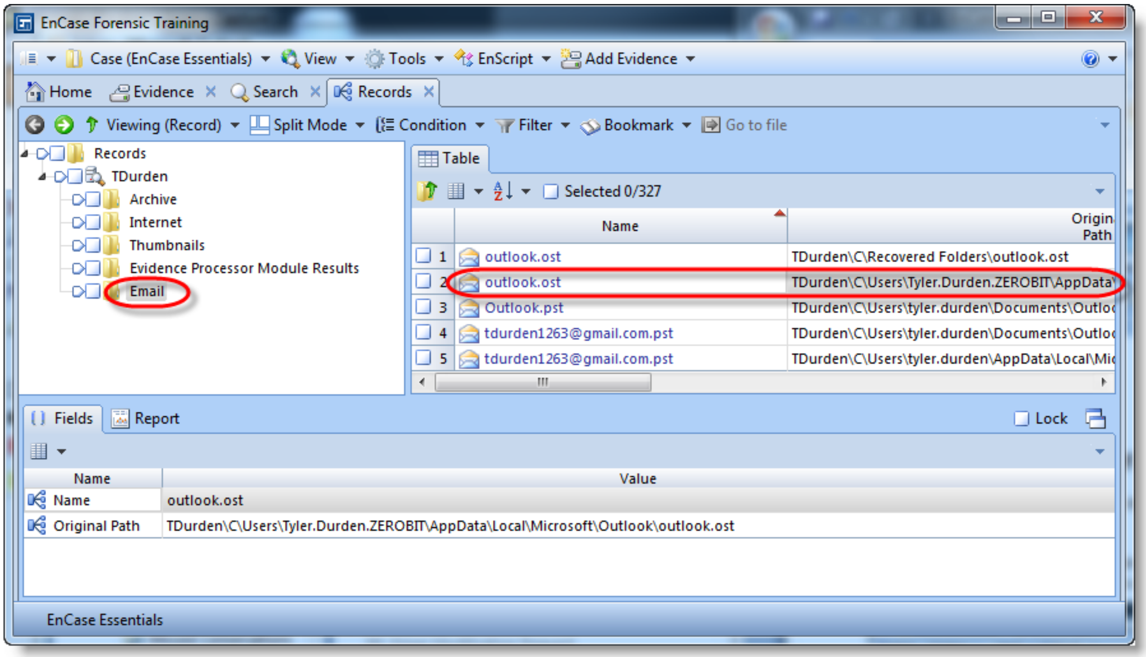


Figure 8-2 View→Records

A list of processed e-mail archives will be displayed under the Email folder. To open an e-mail archive, click on the hyperlink of the name of the archive.



	Name	Origin Path
□ 1	outlook.ost	TDurden\C\Recovered Folders\outlook.ost
□ 2	outlook.ost	TDurden\C\Users\Tyler.Durden.ZEROBIT\AppData\
□ 3	Outlook.pst	TDurden\C\Users\tyler.durden\Documents\Outloo
□ 4	tdurden1263@gmail.com.pst	TDurden\C\Users\tyler.durden\Documents\Outloo
□ 5	tdurden1263@gmail.com.pst	TDurden\C\Users\tyler.durden\AppData\Local\Mic

Name	Value
Name	outlook.ost
Original Path	TDurden\C\Users\Tyler.Durden.ZEROBIT\AppData\Local\Microsoft\Outlook\outlook.ost

Figure 8-3 Click on the e-mail name hyperlink "outlook.ost"